HELSINGIN KAUPPAKORKEAKOULU

Yrityksen tietojärjestelmät

TIETOTURVALLISUUS HAJAUTETUSSA JÄRJESTELMÄSSÄ - VALTIONTAKUUKESKUKSEN TIETOJÄRJESTELMÄN SUOJAAMINEN

Helsingin
Kauppakorkeakoulun
Kirjasto

6269

Tietojärjestelmätiede: yrityksen tietojärjestelmät pro gradu - tutkielma

Matti Laamanen

Kevätlukukausi 1995

9

Johtamisen laitoksen

laitosneuvoston kokouksessa 7 . 6 .19 95 hyväksytty

arvosanalla non sine laude approbatur

KTT Timo Saarinen KTM Eero Larmola

(allekirjoitukset)

HELSINGIN KAUPPAKORKEAKOULU TIIVISTELMÄ

Tietojärjestelmätiede : yrityksen tietojärjestelmät
pro gradu -tutkielma
Matti Laamanen 30.1.1995

TIETOTURVALLISUUS HAJAUTETUSSA JÄRJESTELMÄSSÄ - VALTIONTAKUUKESKUKSEN TIETOJÄRJESTELMÄN SUOJAAMINEN

Tutkimuksen tavoitteet

Tutkimuksessa pyrittiin selvittämään millaisia muutoksia tietojenkäsittelyn ja tietojärjestelmien hajauttaminen tuo atk-järjestelmien turvallisuuteen ja uhkiin. Samalla kartoitettiin Valtiontakuukeskuksen tietojärjestelmän tietoturvallisuutta ja pyrittiin luomaan puitteet tietoturvapolitiikan sekä tietoturvasuunnitelmien luomiselle.

Lähdeaineisto

Lähdeaineistona käytettiin tietoturvan kohteiden ja perusteiden määrittämiseen alan kirjallisuutta ja seminaarijulkaisuja, joita myös sovellettiin Valtiontakuukeskuksen tietojärjestelmään. Valtiontakuukeskuksen tietojärjestelmää kartoitettiin eri järjestelmän kehittämisprojektien yhteydessä ja tarkasteltiin olemassa olevia järjestelmiä sekä strategioita tietoturvallisuuden näkökannalta.

Tutkimuksen tulokset

Tutkimuksessa luodaan kuvaus tietojenkäsittelyn hajauttamisen aiheuttamista muutoksista tietoturvassa ja sen toteuttamisessa tietoturvan kohdealueittain. Samoin luodaan puitteet yrityksen tietoturvan kartoittamiselle, tietoturvapolitiikan ja tietoturvan toteuttamiselle yrityksessä, kartoitetaan yrityksen kannalta merkittävät tietoturvaan liittyvät näkökohdat yrityksen toiminnan ja tietojenkäsittelyn aseman kannalta sekä analysoidaan tietoturvaan vaikuttavia osatekijöitä. Kartoitukseen perehdytään yrityksen tietojärjestelmään ja kartoitukseen liittyen laaditaan kohdeyritykselle kuvaus tietojärjestelmästä tietoturvallisuuden näkökohdasta, esitetään ehdotukset tietoturvapolitiikan ja tarvittavan ohjeistuksen toteuttamisesta sekä todetaan tietoturvassa havaitut puutteet ja tarvittavat toimenpiteet tilanteen korjaamiseksi.

Avainsanat tietoturva, tietoturvapolitiikka, hajauttaminen, suojaaminen

SISÄLTÖLUETTELO

KUVIOIDEN LUETTELO

1
JOHDANTO

Tietotekniikan painopiste on useissa yrityksissä siirtynyt talouden ja hallinnon rutiinijärjestelmistä operatiivista toimintaa palveleviin järjestelmiin, jotka voivat olennaisesti parantaa toiminnan ohjattavuutta ja tuottavuutta sekä luoda uusia valmiuksia päätöksenteolle. Tietojärjestelmät voivat muuttaa jopa kokonaisten toimialojen rakennetta ja kilpailuvoimia, ja luoda yksittäiselle yritykselle huomattavan kilpailuedun muihin alan yrityksiin nähden.[1]

Tietojenkäsittelyn hajauttaminen, tietoliikenteen hyödyntäminen sekä yhä laajeneva atk-palvelujen hyväksikäyttö lisäävät jatkuvasti atk-käyttäjien ulkoista riippuvuutta ja tietojenkäsittelyn turvallisuudelle asetettavia vaatimuksia. Samalla, kun riippuvuus tietojärjestelmistä, tietokoneista, tietoliikenneverkoista ja muista oheislaitteista kasvaa, lisääntyy myös haavoittuvuus käytön häiriöihin tai sen keskeytymisiin nähden. Yrityksen operatiivisen ja tietohallinnon johdon onkin entistä enemmän kehitettävä tietojenkäsittelyä yrityksen toiminnan jatkuvuuden ja koko toiminnan kriittisenä voimavarana.[2]

Useimmat nykyisin käytössä olevat tietoturvamallit perustuvat vanhaan "keskusjohtoiseen" tietohallintoon, jossa esim. laitteiston useimmiten oletettiin koostuvan pelkästään keskustietokoneeseen yhteydessä olevista päätteistä. Vielä kymmenkunta vuotta sitten oli tietokonejärjestelmä suhteellisen helposti suojattavissa, koska järjestelmä oli kokonaisuudessaan saman rakennuksen sisällä tai ainakin saman organisaation tiloissa. Nykyään tilanne on monimutkaisempi. Tietojärjestelmät ovat kasvaneet hyvin suuriksi ja on mahdollista siirtää tietoja tietojärjestelmästä toiseen.[3]

---

[1] Hannus, s. 1

[2] Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu, s.1

[3] Ekberg, s. 7

Tietokoneiden ja tietojärjestelmien yleistyessä kasvaa samalla sellaisten ihmisten määrä, jotka osaavat käyttää niitä ja tuntevat tietokoneen ja tietojärjestelmien toimintaperiaatteita. Kun aikaisemmin tietokoneiden väärinkäyttöön pystyi vain pieni rajattu ryhmä, nykyisin miltei kuka tahansa pystyy aiheuttamaan jonkin asteista vahinkoa tietojärjestelmälle. Samoin mahdollisuudet tietokoneen värinkäyttöön kasvavat tietokoneiden lukumäärän kasvaessa ja niiden käytön levitessä kaikkialle yhteiskuntaelämän eri aloille.

1.1 Tutkimuksen tausta ja tavoitteet

Tutkimuksen ensimmäisen vaiheen tavoitteena on kuvata niitä uusia ongelmia ja uhkia, joita tietojärjestelmien käytön yleistyminen ja tietojenkäsittelyn hajauttaminen: älykkäiden päätteiden, henkilökohtaisten tietokoneiden ja itsenäiskäytön lisääntyminen sekä tietoverkkojen nopea kasvu tuo tietoturvan toteuttamiselle, ja joihin ei perinteisillä keskitettyyn tietojärjestelmään pohjautuvilla suojatoimilla täysin pystytä vastaamaan.

Tutkimuksen toisena kohteena on tietoturvallisuuden kartoitus yrityksessä. Tutkimuksessa pyritään löytämään keinoja, joilla voidaan kartoittaa yrityksen haluttu tietoturvallisuuden taso ja kartoittaa tarvittavat toimenpiteet sen saavuttamiseksi. Kartoituksen lähtökohtana on muutos keskitetystä tietojärjestelmästä hajautettuun tietojärjestelmään, mutta tarkoituksena on kuvata myös yleisesti tietoturvan puitteita organisaation atk-järjestelmien suojaamisessa. Kartoituksen avulla pyritään luomaan kokonaiskuva tietojärjestelmästä ja sen tietoturvasta ja antaa näin yritykselle pohja tietoturvan toteuttamiselle ja kehittämiselle pitemmällä tähtäimellä.

Tutkimuksen tuloksina luodaan kuvaus tietojenkäsittelyn hajauttamisen aiheuttamista muutoksista tietoturvassa ja sen toteuttamisessa tietoturvan kohdealueittain. Samoin luodaan puitteet yrityksen tietoturvan kartoittamiselle, tietoturvapolitiikan ja tietoturvan toteuttamiselle yrityksessä, kartoitetaan

yrityksen kannalta merkittävät tietoturvaan liittyvät näkökohdat yrityksen toiminnan ja tietojenkäsittelyn aseman kannalta sekä analysoidaan tietoturvaan vaikuttavia osatekijöitä. Kartoituksen avulla perehdytään yrityksen tietojärjestelmään ja kartoitukseen liittyen laaditaan kohdeyritykselle kuvaus tietojärjestelmästä tietoturvallisuuden näkökohdasta, esitetään ehdotukset tietoturvapolitiikan ja tarvittavan ohjeistuksen toteuttamisesta sekä todetaan tietoturvassa havaitut puutteet ja tarvittavat toimenpiteet tilanteen korjaamiseksi.

1.2 Tutkimuksen rajaus

Tässä tutkimuksessa yhteydessä tietoturva tarkoittaa lähinnä tietojen, tietovälineiden sekä tietojenkäsittelyn suojaamista mahdollisia uhkia vastaan. Kuitenkin tietojenkäsittelyn ja informaatiojärjestelmien merkityksen kasvaessa tietoturva tulee nähdä myös laajemmassa merkityksessä. Tällöin tietoturvallisuuteen kuuluvat yrityksen kaikki atk-tietojärjestelmät, tietovirrat, tietojen eheys ja muut yrityksen tietojärjestelmien toimintaan liittyvät seikat. Samalla on huomioitava, että vaikka usein virheellisesti käytetään "tietosuoja"-nimitystä tarkoitettaessa tietoturvaa, määritellään tietosuoja kuitenkin henkilön yksityisten tietojen loukkaamattomuudeksi eli yksityisyydeksi (engl. privacy), eikä se sellaisena kuulu tutkielman aihepiiriin.

Organisaation tietojärjestelmällä tarkoitetaan tässä tutkimuksessa organisaation informaatiosysteemiä kokonaisuudessaan, sen toimintatapoja ja yhteyksiä muihin järjestelmiin. Atk-järjestelmällä tarkoitetaan lähinnä edellisen atk-teknistä toteutusta, joka organisaatiosta ja järjestelmän toteutustavasta riippuen kattaa tietojärjestelmän kokonaan tai osittain. Käsitteinä atk-järjestelmä ja tietojärjestelmä tarkoittavat hyvin pitkälle samoja asioita, koska ero on lähinnä tarkastelunäkökulmassa, ja usein niitä käytetäänkin samassa merkityksessä.

1.3
Tutkimuksen rakenne

Aihetta lähestytään kuvaamalla ensin tietoturvan tavoitteita ja sen kohteita lähinnä perinteisen tietoturvanäkemyksen pohjalta, jonka mukaan tietojärjestelmän suojattavat kohteet jaetaan seuraaviin alakohtiin:[4]

1. Fyysinen suojaus
2. Laitteistojen suojaus
3. Käyttöjärjestelmän suojaus
4. Tiedon suojaus
5. Tiedonsiirron suojaus

Samalla esitetään niitä erilaisia toimenpiteitä ja keinoja, joilla tietoturvaa pyritään toteuttamaan sekä toisena vaiheena tutkitaan hajautetun tietojenkäsittelyn aiheuttamia muutoksia tietoturvallisuudessa ja sen toteuttamisessa. Hajautus muuttaa ja luo uusia uhkia ja vaikuttaa sitä kautta tietoturvan kohteisiin. Keskitetyn tietojärjestelmän tietoturvatoimet eivät välttämättä vastaa hajautuksen tuomiin uusin haasteisiin. Perinteiseen atk-turvallisuuteen kuuluvat toimenpiteet ovat suhteellisen passiivisia ja turvallisuusongelmat melko staattisia ja kuitenkin järjestelmän haavoittuvuus aiheutuu usein teknologian, sovellusalueiden ja informaatiojärjestelmien jatkuvasta muutoksesta.[5]

Yrityksen tietoturvan kartoituksessa lähdetään liikkeelle selvittämällä tietojärjestelmän asema yrityksessä, sen merkitys yrityksen toiminnalle sekä tietojenkäsittelylle asetetut tavoitteet. Samalla pyritään saamaan kuva tietojärjestelmästä kokonaisuutena; laitteistosta ja toiminnasta. Seuraavaksi perehdytään tietoturvallisuuteen yleisellä tasolla (tietoturvan kohteet ja tavoitteet sekä sen merkitys tietojärjestelmän ja yrityksen toiminnalle) ja keskitytään tarkastelemaan yrityksen tietoturvallisuuden toteutusta kohteittain.

---

[4] Ekberg, s. 7

[5] Tate, s.58

Tämän jälkeen pyritään löytämään ne eri osa-alueet, jotka vaikuttavat yrityksen tietojärjestelmän tietoturvan tasoon. Samoin pyritään hahmottamaan tietoturvapolitiikan suuntaviivoja, tehdään ehdotukset käyttäjien ja osastojen ohjeistuksesta ja tietoturvallisuutta koskevista säännöistä.

Seuraavaksi käsitellään riskien hallintaa atk:ssa ja riskianalyysien tarpeellisuutta yrityksissä sekä kyselytutkimuksen avulla kartoitetaan järjestelmän mahdolliset riskit. Yrityksen informaatiosysteemien strategian määrittelyyn ei nykyisin riitä perinteinen kustannus- ja hyötyajattelu. Pitkälle hajautettu henkilökohtainen tietojenkäsittely, monimutkaiset tietoverkot ja tietokantasysteemit ovat tehneet riskistä kolmannen tekijän informaatiosysteemien suunnittelussa.[6]

Tutkimuksen loppuosassa perehdytään kohdeorganisaation toimintaan, liiketoiminta- ja tietohallintastrategioihin sekä atk-järjestelmään toimintaan ja rakenteeseen. Tältä pohjalta kartoitetaan organisaation tietojärjestelmän tietoturva ja laaditaan tietoturvan kehittämissuunnitelman puitteet.

1.4 Tietoturvakäsitteistöä

Tietoturvan on suhteellisen uusi tietojenkäsittelyn alue ja tästä syystä sen käsitteet ja määritykset ovat varsinkin Suomessa melko puutteelliset. Suomennosten puutteellisuus ja näkemyserot alan asiantuntijoiden kesken on aiheuttanut sen, ettei yhtenäistä käsitteistöä ole vielä käytössä. Sen sijaan useat eri tahot (mm. Tietotekniikan liitto, Helsingin tietojenkäsittely-yhdistys, eräät ministeriöt, puolustusvoimat, eräät yritykset ja yksityiset konsultit) ovat luoneet omat oppaansa ja käsitteistönsä.

Tätä tutkielmaa tehtäessä englanninkielisistä lähdeteoksista peräisin olevissa viitteissä käytetään seuraavia suomennoksia:

---

[6] Tate, s.58

privacy = yksityisyys, tietosuoja

data security = tietojen (data) suojaus, vrt. tiedon eheys

computer security, EDP security = atk-turvallisuus, lähinnä laitteiden fyysinen suojaus

information (system) security = tietojärjestelmien turvallisuus, tietoturvallisuus (laajemmassa merkityksessä tietojärjestelmien ja kaikkien sen osien; toimintojen, laitteiden, ohjelmien, tietojen, yhteyksien jne. turvallisuus)

Muita tutkielmassa käytettäviä käsitteitä:

atk-riski = atk-toiminnan fyysiseen ominaisuuteen-, ohjelmistoon tai henkilöstöön liittyviä vahingon vaaroja, jotka toteutuessaan aiheuttavat taloudellisia menetyksiä[7]

tiedon eheys = tietojen oikeellisuus, luotettavuus, alkuperäisyys

tiedon luottamuksellisuus = salaisen tiedon käytön valvonta ja rajoittaminen

tiedon saatavuus (=käytettävyys) = järjestelmän tuottaman ja siihen talletetun tiedon ja palveluiden on oltava hyödynnettävissä hyväksyttävässä ajassa

tietosuoja = tiedon loukkaamattomuus, yksityisyys

tietokonevirus = ohjelma, joka kopioi itsensä muihin ohjelmiin ja/tai aiheuttaa vahinkoa tietokoneelle, sen ohjelmille, tiedostoille ja/tai tiedoille

tietoturvallisuus = tietojen, järjestelmien ja palveluiden asianmukainen suojaaminen normaali- ja poikkeusoloissa

2
HAJAUTUKSEN VAIKUTUS TIETOTURVAAN JA SEN TOTEUTTAMISEEN

Useimmilla tietojenkäsittelyosastoilla ei ollut tietoturvallisuuden ja yksityisyyden suojan hoitotoimia ennen vuotta 1980, lukuunottamatta sotilaallisia, diplomaattisia tai muita vastaavan tyyppisiä organisaatioita. 1980-luvulle tultaessa turvallisuus muodostui yhä tärkeämmäksi, koska integroitujen tietokantojen takia yhä suurempi määrä organisaation elintärkeistä tiedoista oli

[7] Atk-riskit ja niiden hallinta s.4

nyt saatavissa suorakäyttöisesti[8]. Nykyisin tietojenkäsittelyn ja tietojärjestelmien hajauttaminen ovat tuoneet uusia näkökulmia atk-turvallisuuteen ja sen toteuttamiseen. Hajautuksen lisäksi selvä kehityssuunta on myös eri organisaatioiden halu kytkeä tietojärjestelmät yhteen tietoverkkojen avulla molempia osapuolia kiinnostavien tietojen vaihtamiseksi.

2.1 Tietoturvan tavoitteet

Informaatiosysteemien kehitys on tuonut yrityksille merkittäviä etuja, mutta se on myös luonut uusia ongelmia ja riskejä. Yritysten yhä kasvava riippuvuus informaatiosysteemeistä on tehnyt ne uudella tavalla haavoittuviksi[9].

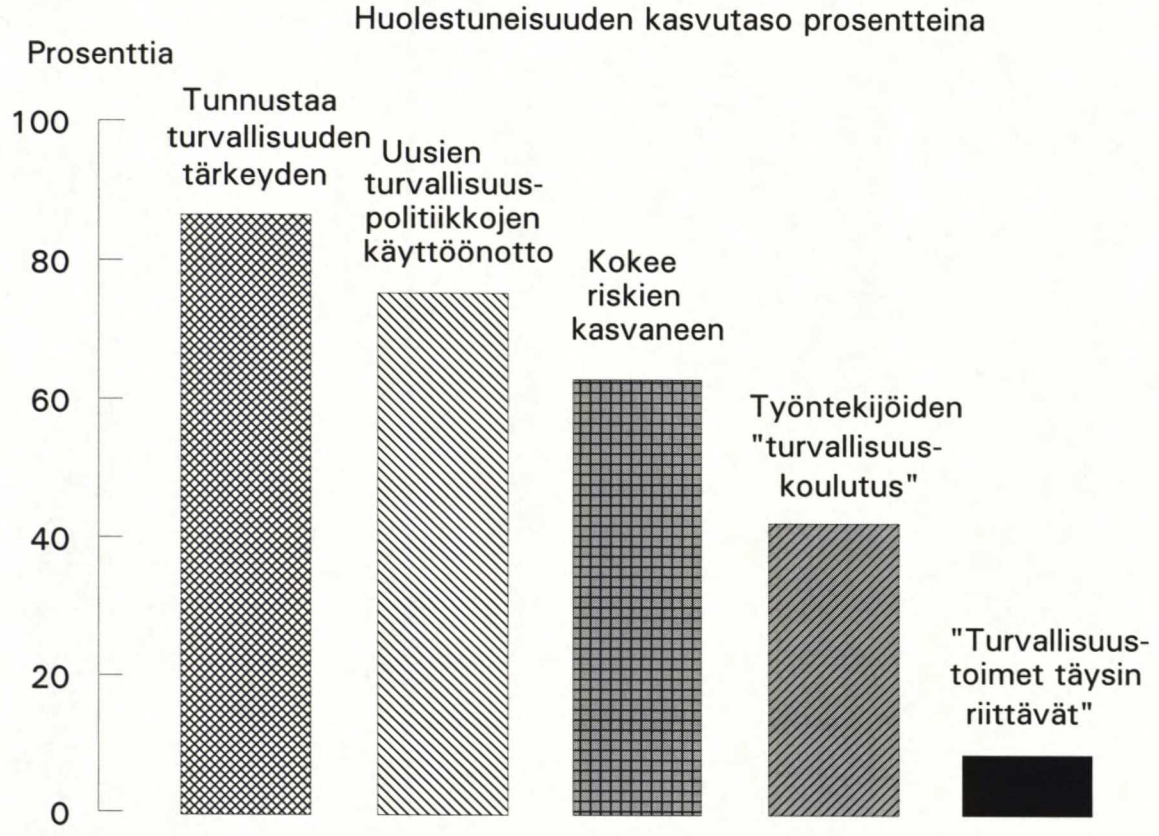
Haavoittuvuudella tarkoitetaan tietojenkäsittelyn yhteydessä sitä kuinka helposti tietoja voidaan väärinkäyttää tai niitä seikkoja, joiden vuoksi tietoja ei voida käyttää aiotulla tavalla, esimerkiksi tiedot eivät ole saatavilla, ne ovat virheellisiä tai tallennettuja tietoja käytetään väärin. Haavoittuvuusriskien hallinta ja yrityksen kriittisen, salaisen tiedon suojaaminen ovat välttämättömiä laajentuneessa ja hajautuneessa tietojenkäsittelyjärjestelmässä.

---

[8] Booth, s.276

[9] Tate, 1988 s.58

Kuvio 1 Haavoittuvuuden tiedostaminen yrityksissä



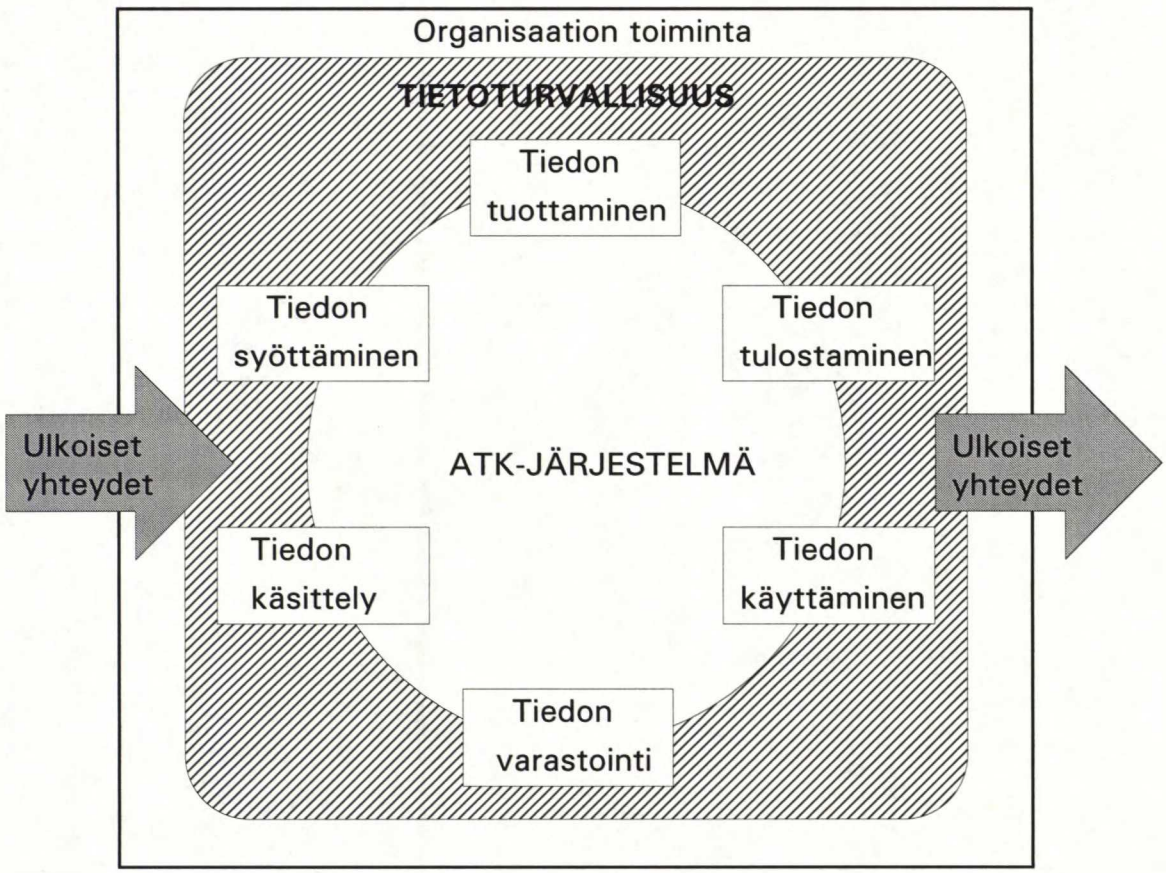
Lähde: Ernst And Whinney, U.S. Computer Security Survey 1987

Kuviossa 1 on esitetty yrityksien haavoittuvuuden tiedostamisen kasvun jakautuminen eri osa-alueille. Huomattavaa on että, alle 10 % yrityksistä piti turvatoimiaan täysin riittävinä, kun taas yli 60 % tutkimukseen osallistuneista yrityksistä koki riskien selvästi kasvaneen.

Tietojenkäsittelyn varmistaminen on myös yksi tuotantotoiminnan jatkuvuuden ratkaisevista perusedellytyksistä. Myös atk-laitteisiin sekä tietovarastoihin sitoutuneen pääoman kasvun tulisi kiinnittää yritysten huomion tietoturvallisuuteen ja sen toteuttamiseen. Yleistäen tietoturvallisuuden kehittämisen päätavoitteena voidaan pitää hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuuden luomista, joka mahdollistaa tietojärjestelmän ja organisaation toiminnan niin normaali- kuin poikkeusoloissakin.

Atk-toiminnan turvaamisella tarkoitetaan tietojärjestelmien turvallisuuden kehittämistä poistamalla tai pienentämällä mahdollisten virheiden, väärinkäytösten ja atk-laitteiden häiriöiden ja fyysisten vahinkojen sattumismahdollisuuksia tai varautumalla niihin ennakolta.[10]

Kuvio 2 Tietojen turvaaminen



Juhani Saaren määritelmän mukaan tietoturvallisuus sisältää tiedon oikeellisuuden, loukkaamattomuuden, suojaamisen, valtuutetun käytön ja luottamuksellisuuden lähtien tiedon tuottamisesta, syöttämisestä tietokoneille, automaattisesta ja manuaalisesta käsittelystä ja päätyen tulostukseen, varastointiin ja lopulta tiedon käyttämiseen. Määrittely kattaa tietoturvalle asetettavat vaatimukset kaikissa tietojenkäsittelyn eri vaiheissa, alkaen tiedon

[10] Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu s.4

tuottamisesta tai sen syöttämisestä järjestelmään ja päätyen tiedon varastointiin tai sen loppukäyttöön.

Tietojärjestelmien tiedon suojauksen suunnittelussa on lähdettävä siitä, että ensin selvitetään suurimmat tietoa uhkaavat vaarat. Näitä voivat olla esim. tulipalo, laitteistoviat, sähköhäiriöt ja ihmisten toiminta.[11] Riippumatta järjestelmän koosta tai sen luonteesta tulisi tietoturvan toteutuksessa pyrkiä seuraaviin tavoitteisiin:

-käsiteltävän tiedon luottamuksellisuus
-tiedon ja käsittelyn oikeellisuus
-systeemien, tietojen ja palvelujen saatavuus
-tietojenkäsittelyn tarkastettavuus[12]

Atk-turvallisuuden päätehtävä on yrityksen toiminnan kannalta elintärkeiden atk-järjestelmien ja tietoliikenneyhteyksien suojaaminen sekä atk-palvelujen ja -materiaalien saannin varmistaminen siten, että toimintaa voidaan häiriöistä ja vahingoista huolimatta jatkaa ennalta hyväksytyllä toiminnan tasolla sekä keskeytyksen jälkeen mahdollisimman nopeasti palauttaa tietojenkäsittely yrityksen kokonaistoiminnan vaatimalle tasolle.

Tietojenkäsittelyn turvaamisen tarpeet voidaan jakaa yrityksen normaalien toimintaolosuhteiden vaatimiin turvallisuustoimenpiteisiin ja toiminnan varmistamiseen poikkeusoloissa. Poikkeusoloilla tarkoitetaan tässä yhteydessä sellaisia häiriötilanteita, joiden syntyyn yritys ei itse voi vähäisimmissäkään määrin vaikuttaa. Tällaisia ovat mm. atk-varaosien saannin tyrehtyminen, kauppapoliittiset rajoittamistoimenpiteet ja vakavat kriisitilanteet.

Tietojärjestelmien kehittyessä ja organisaation toiminnan tulessa yhä riippuvaisemmaksi niiden toiminnasta, on yhä vaikeampi tehdä eroa toimintavarmuudelle asetetuista vaatimuksista tai niiden eroista

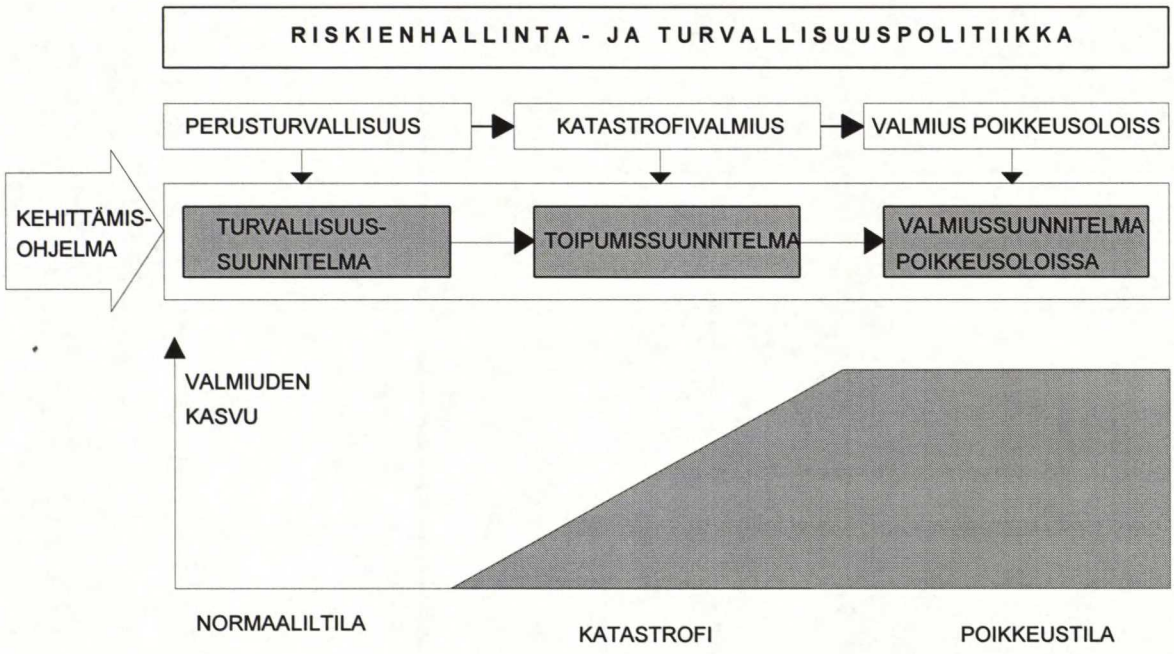
---

[11] Uusitupa, 1989 s. 54

[12] Saari, s. 163

normaalioloissa ja poikkeusoloissa. Poikkeusolojen toimintaan varautumista kiireellisempää on ehkäistä normaalioloissa sattuvat vahingot ja häiriöt. Samalla luodaan edellytykset poikkeusolojen valmiudelle.

Kuvio 3 Tietojenkäsittelyn turvaamisen osa-alueet



Lähde: Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu s. 5

Tietojenkäsittelyn turvallisuustoimenpiteet ovat pitkälti samat ajateltiinpa normaaliaikojen toiminnan varmistamista tai kykyä jatkaa toimintaa poikkeustilanteessa. Toiminnan jatkuvuuden varmistaminen muodostaakin yhtenäisen valmiussuunnitelman perusturvallisuudesta katastrofivalmiuden kautta valmiuteen järjestelmän toiminalle poikkeusoloissa. Atk-valmiussuunnittelun kokonaistavoitteina voidaankin pitää tietojenkäsittelyn perusturvallisuuden luomista ja häiriöiden ennaltaehkäisyä, varautumista katastrofien aiheuttamien vahinkojen rajoittamiseen, toiminnan jatkamiseen ja normaalitoiminnan palauttamiseen sekä toimintavalmiuden luomista myös poikkeusoloissa.

2.2
Tietoturvan perinteiset kohteet

Tarkasteltaessa atk-järjestelmää tietoturvan näkökulmasta voidaan se jakaa erilaisiin turvattaviin kohteisiin. Perinteisesti on lähdetty liikkeelle järjestelmän fyysisestä suojaamisesta, tavoitteena atk-tilojen ja laitteiden suojaaminen esim. tulipalolta. Tietojärjestelmän suojattavat kohteet voidaan jakaa yleisesti seuraaviin alakohtiin:[13]

1. Fyysinen suojaus (rakennusten suojaus, vahinkojen ennakointi jne.)
2. Laitteistojen suojaus (muistien ja päätelaitteiden suojaus, ajonaikainen suojaus, toiminnan seuranta jne.)
3. Käyttöjärjestelmän suojaus (pääsyn valvonta, sisäänkirjautuminen, virtuaalikoneratkaisut, suojausluokat jne.)
4. Tiedon suojaus (tiedon virheettömyyden testaus, suojatut muistialueet, tietokannan suojaus jne.)
5. Tiedonsiirron suojaus (tiedon suojaus päätteissä, verkon suojaus, tiedonsiirron suojaus, koodien murtamisuhat jne.)

Edellä esitetyt tietoturvan kohteet löytyvät yleisesti ottaen kaikista tietojenkäsittely-ympäristöistä. Eri kohteisiin voidaan suunnata erilaisia toimenpiteitä ja menetelmien kohteen tietoturvan parantamiseksi. Kohdejakoa voidaan tarkentaa ja liittää kuhunkin kohteeseen siihen kuuluvia tietoturvatekijöitä ja toimenpiteitä:

1. Fyysinen suojaus

kohde:

-atk-tilat, atk-laitteet ja apulaitteet, ohjelmistot, tietovarastot, tietoliikennelaitteet

---

[13] Ekberg, s. 7

toimenpiteet:

-rakenteellinen suojaus, palotorjunta, vesivahinkojen torjunta, sabotaasin ja ilkivallan ehkäisy, valvontalaitteet/vartiointi, tietovarastojen ja ohjelmistojen säilytystilat

2. Toiminnan varmistaminen

kohde:

-atk-laitteet + apulaitteet, sähkönsyöttö, tietoliikenne, avainhenkilöt

toimenpiteet:

-varmuuskopiointi, laitteistohuolto, laitteistovarmennukset, UPS, koulutus, varamiesjärjestelyt

3. Laadun varmistaminen

kohde:

-ohjelmistot, tiedot, tietojärjestelmien kehittäminen, käyttö, palvelut

toimenpiteet:

-työn organisointi, työmenetelmät ja työkalut, tiedon, ohjelmien, toimintojen ja tulosten tarkastus, testaus, dokumentointi, laadunvalvonta, hyväksymismenettelyt, virheiden poistaminen ennen tuotantoa

4. Tietosuoja

kohde:

-ohjelmistot, tiedot, tietokoneet, asiakirjat, tulosteet yms. paperit

toimenpiteet:

-valtuutusjärjestelmä, salasananhallinta, käytön seuranta ja poikkeamien raportointi, ohjelmalliset tarkistukset, varusohjelmiston suojaus- ja muiden ominaisuuksien käyttö, suojausohjelmistot, tiedon salaaminen

5. Tietoliikenteen suojaus

kohde:

-päätejärjestelmät, tietoliikenne, tietokoneverkosto

toimenpiteet:

-verkon valvonta, siirtovirheiden tarkkailu, salakirjoitus, yhteydenottoprotokollat, vastasoitto-periaate, lukot

6. Valmiussuunnittelu ja varajärjestelmä

kohde:

-merkittävät tietojärjestelmät

toimenpiteet:

-katastrofitilanteiden toiminnan suunnittelu, organisointi ja vastuu, varatilat, -koneet ja -laitteet, laitteisto-, ohjelmisto-, ja tiedostoluettelot, kriittisten toimintojen ensivalmius

2.2.1

Fyysinen suojaus ja laitteistojen suojaus

Tärkein tai ainakin vanhin tapa keskitetyssä atk:ssa on fyysinen suojaus ja se on myös suhteellisen helppo toteuttaa. Tietokonelaitteistojen sijoitusta suunniteltaessa on huomioitava useita seikkoja. Ensinnäkin sijoituspaikan tulisi olla suojassa luonnon aiheuttamilta uhkatekijöiltä. Tällaisia uhkia ovat mm. tulvat, maaperän heikkolaatuisuus, myrskyt, salamat, lumi ja jää. Edelleen laitteistot tulee sijoittaa paikkaan, missä tarvittavat palvelut ovat helposti saatavilla. Tällaisia palveluja ovat kuljetusyhteydet, posti- ja telepalvelut, sähkö, vesi ja viemäröinti. Lisäksi sijoittamisessa on varottava naapuriston aiheuttamia vaaroja. Tällaisia voivat olla tulenarat ja räjähdysalttiit toiminnot, syövyttävien ja myrkyllisten aineiden varastot tai kuljetus, pöly, tärinä, vilkas liikenne tai suurteholähettimet ja tutkat. Rauhaton ympäristö voi myös aiheuttaa ilkivaltaa, jolloin on syytä järjestää toiminta siten, että se ei erotu erityisesti ympäristöstään ja siten kiinnitä tarpeetonta huomiota.

Suojautuminen kannattaa ulottaa riittävän etäälle. Mikäli mahdollista, tietojenkäsittelylaitteiston sijoitusrakennus kannattaa suojata hälytysjärjestelmällä. Keskuslaitteisto suositellaan sijoitettavaksi maanalaisiin tai rakenteellisesti hyvin suojattuihin tiloihin. Jollei tämä ole mahdollista, pitää laitteisto sijoittaa ikkunattomaan tilaan ja normaalit kulkureitit on voitava

sulkea tehokkaasti. Rakenteiden ja laitteiden asennustelineiden on oltava riittävän lujia kestämään laitteiden kokonais- ja pistekuormia. Laitteiston sijoitustilat on suunniteltava riittävän suuriksi sillä ne pyrkivät ajan kuluessa täyttymään. Varsinkin laitteiston vaihdon yhteydessä, kun uusi ja vanha laitteisto ovat sijoitettuna samaan tilaan, voi syntyä vaaratilanteita.

Toimistoympäristössä mahdollisuudet erikoisjärjestelyihin ovat pienemmät. Tällöinkin laitteisto voidaan sijoittaa siten, että sijoitushuone voidaan työajan jälkeen lukita. Tällöin tietotaltiot kuten levykkeet ja nauhat jäävät samaan lukittuun tilaan ja niille kannattaa hankkia vahva paloturvakaappi, joka samalla toimii murtosuojana.

Tavallisimpia turvatoimia laitteiston suojauksessa ovat seuraavat:

- tietokone sijoitetaan erilliseen vartioituun konehuoneeseen
- tietokonetta suojellaan tulipalolta, vesi- tai muilta nestevahingoilta rakenteellisesti sekä hälytys- ja sammutusjärjestelmillä
- ilmankosteutta ja lämpötilaa valvotaan
- taataan häiriötön sähköjärjestelmä[14]
- varmuuskopiot säilytetään turvallisissa paikoissa
- jokaisen päätteen tilasta ja käyttäytymisestä pidetään kirjaa[15]

Fyysisen suojauksen piiriin kuulu myös kiinteistön yleinen vartiointi, jolla pyritään kontrolloimaan rakennukseen pääsyä ja siellä liikkumista sekä estämään asiaton pääsy yrityksen tiloihin. Esimerkiksi asiakaspalvelua harjoittavan yrityksen kiinteistö on jaettavissa kolmeen valvontavyöhykkeeseen:[16]

1. vyöhyke: asiakastilat
2. vyöhyke: muut normaalikäytössä olevat tilat
3. vyöhyke: erikoissuojelua vaativat tilat, kuten:
   - atk-käytön tilat

---

[14] Ledell ym, s. 18

[15] Ekberg, s. 8

[16] Tietosuojan toteuttamisohjeet, s. 16

- tietokonepäätteiden tilat
- rekisteri- ja arkistointitilat
- varmistus, arvopaperi ym. holvit

2.2.2 Käyttöjärjestelmän ja tiedon suojaus

Varsinkin viime aikoina on käyttöjärjestelmän ja itse tietokoneen suojauksessa kiinnitetty huomiota suojautumiseen murtautujia vastaan. Eräitä suojakeinoja ovat esimerkiksi vastasoittolaite, joka estää (teoreettisesti) pääsyn tuntemattomasta verkkoliitännästä tietokonejärjestelmään sekä pääsyn valvontalaitteet monimutkaisine tunnistusmenettelyineen, joiden kautta ulkoa tulevat kutsut tulevat tietokoneverkkoon.

Tietokoneen muistin suojauksella tarkoitetaan sitä, ettei ohjelma ylitä sille varattua muistialuetta ja toisaalta, että muistissa olevat ohjelmat ja tiedot pysyvät salassa. Muistin suojaamiseksi voidaan esimerkiksi tarkistaa, että käyttöjärjestelmä nollaa muistialueen ohjelman suorituksen jälkeen, muistialueen ylitys on estetty (käyttöjärjestelmä- tai laiteominaisuus) ja että salaisissa tapauksissa muiden ajojen suorittaminen samaan aikaan estetään ja tyhjennetään käyttöjärjestelmää lukuunottamatta koko muisti.

Ohjelmien ja käyttöjärjestelmän suojaukseen voidaan käyttää hyväksi myös niiden tarjoamia erilaisia palveluja ja tarkistuksia, joiden avulla voidaan valvoa ja rajata käyttäjien valtuuksia. Käyttöoikeuksien myöntämisen jälkeen voidaan myös tarkkailla toimintoja ja resurssien käyttöä.[17] Tietovälineiden ja tiedostojen käytössä on käyttövaltuuksista pidettävä tarkoin huolta, jotta esim. ei vahingossa tuhota tiedostoja, joita muut atk-käyttäjät tai ohjelmat tarvitsevat. Samalla on pystyttävä rajoittamaan tietojen käyttöä niin, ettei tiedot joudu luvattomille käyttäjille.

Tärkeimpiä tiedon turvaamistoimia ovat selvien toimintaohjeiden laatiminen sovellusten normaalikäyttöön sekä selvien ennalleenpalautus ja

---

[17] Tietosuojan toteuttamisohjeet, s. 14, 15

uudelleenaloitusohjeiden laatiminen. Erittäin tärkeää on myös tiedostojen varmuuskopiointi. Varmuuskopioinnissa on varmistauduttava, että mahdolliset virheet kopioitavissa tiedostoissa havaitaan ennen kuin varmuuskopionauha tai -levy vapautetaan uudelleen käytettäväksi. Varmuuskopiot on säilytettävä erillään muista atk-tiloista ja niiden säilytyspaikan on oltava palo- ja murtosuojattu. Samoin dokumenteista on oltava ajan tasalla olevat kopiot muualla kuin atk-tiloissa. Sovellusdokumenttien lisäksi on varmistettava myös katastrofisuunnitelmien ja poikkeusoloissa noudatettavien ohjeiden säilyvyys.

Tiedon suojauksessa voidaan tiedon suojattavuusaste määritellä esimerkiksi tiedon uusimisen, palauttamisen vaikeuden ja kalleuden perusteella sekä sen mukaan, miten laaja toiminta tiedon tuhoutuessa vaarantuu. Suojattavuusaste voi rakentua esim. lähtien seuraavista luokista:

1. Tiedot, joiden tuhoutuminen vaarantaa sovelluksen ja yrityksen toiminnan jatkumisen
2. Tiedot, joiden tuhoutuminen merkitsee toiminnan keskeytymistä, mutta ei estä toiminnan jatkamista huomattavin ponnistuksin
3. Tiedot, joiden tuhoutumisesta seuraa huomattavia taloudellisia menetyksiä
4. Tiedot, joiden tuhoutumisesta tai muuttamisesta seuraa uhka yksilön/yrityksen oikeuksille

2.2.3
Tiedonsiirron suojaus

Perinteisessä keskitetyssä tietojenkäsittelyssä tiedot toimitettiin lomakkeina, reikäkorteilla tai muilla, uudenaikaisemmilla, tietovälineillä atk-keskukseen. Myös tietovälineiden säilytykseen osattiin kiinnittää huomiota ja vuodot pyrittiin estämään näissä työvaiheissa.[18] Tekniikan kehittyessä luotiin yhteydet etäispäätteisiin, mutta yhteyden suojaukseen ei aluksi osattu kiinnittää huomiota. Vasta myöhemmin tietoverkkojen ja yhteyksien yleistyessä huomattiin niiden alttius vahingoille ja väärinkäytöksille.

---

[18] Uusitupa, 1989 s.55

Datayhteyksien suojaamiseen on perinteisesti pyritty käyttämällä kiinteitä linjoja, jotka ovat yrityksen sisäisiä linjoja tai esim. puhelinyhdistykseltä pysyvästi vuokrattuja linjoja, ja välttämällä yleisiä linjoja. Yhteydenoton laillisuus tarkistetaan avaimen eli koodin mukaan, riippumatta siitä onko kyseessä kiinteä tai yleinen linja taikka koneiden keskinäinen yhteydenpito. Muistettavan avaimen lisäksi voidaan käyttää myös esim. magneettisia tunnuskortteja tai äänen, sormenjälkien tai hahmon tunnistukseen tarkoitettuja erikoislaitteita.[19] Koska linjayhteydet kuitenkin ovat suhteellisen haavoittuvia, on tietojen suojaamiseen käytetty myös salaamislaitteita, joiden avulla voidaan salata sanoma (salakirjoitus) ja ohjaustiedot (linjasalaus).

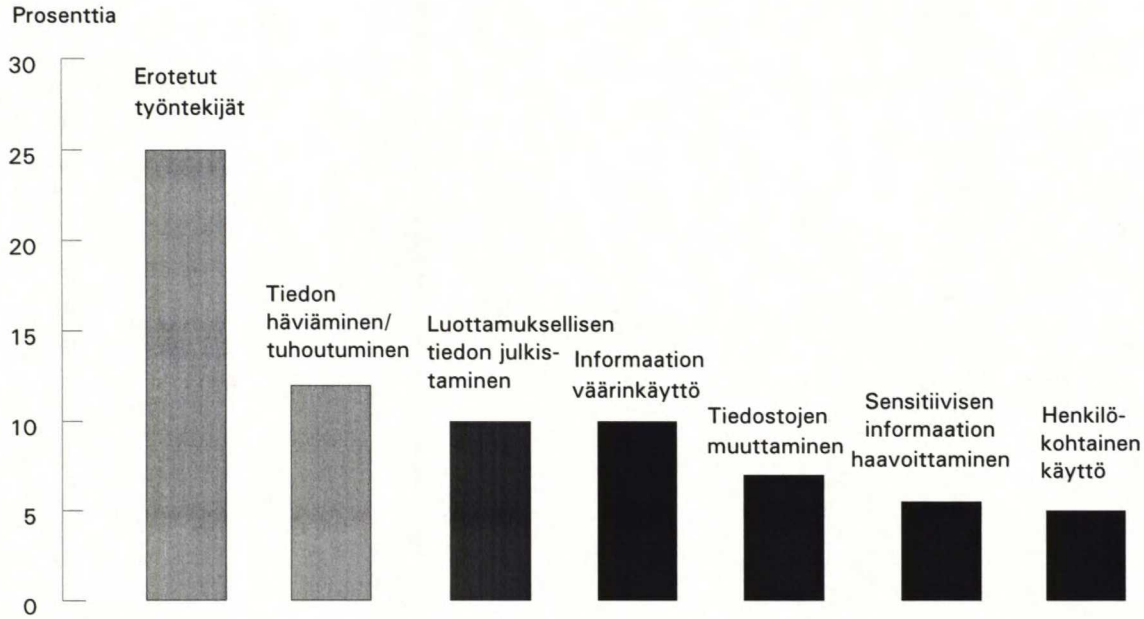
2.3
Hajautuksen vaikutus tietoturvan uhkiin ja toteutukseen

Tietojenkäsittelyn hajauttamisen vaikutus tietoturvan kohteisiin ja tietoturvan toteuttamiseen johtuu niistä uusista tai muuttuneista uhkatekijöistä, jotka mikrotietokoneet, tietoverkot ja itsenäiskäytön lisääminen tuovat tullessaan. Jos yrityksessä on perinteisen kohdejaon perusteella laaditut turvallisuusohjeet ja -toimenpiteet, on kohteet käytävä yksitellen läpi kiinnittäen huomio hajautetun tietojenkäsittely-ympäristön erityispiirteisiin ja niiden vaikutukseen tietoturvallisuuteen.

---

[19] Tietosuojan toteuttamisohjeet, s. 14, 15

Kuvio 4 Ei-rahallisten tappioiden prosenttijakauma



Lähde: Ernst And Whinney, U.S. Computer Security Survey 1987

Kuviossa neljä on kuvattu erään Yhdysvalloissa tehdyn tutkimuksen tuloksena saatu ei-rahallisten vahinkojen prosentuaalinen jakauma. Erotettujen työntekijöiden suuri osuus korostaa henkilökunnan merkitystä tietoturvallisuudessa ja sen toteuttamisessa.

Tietoturvallisuuden tärkeys perustuu sellaisten tietojärjestelmää uhkaavien satunnaisten tai tarkoituksellisten tapahtumien olemassaoloon, jotka voivat vahingoittaa yrityksen tietojärjestelmää tai informaatioresursseja. Tällaisia uhkatyyppejä ovat ympäristöriskit, laitteistohäiriöt, ohjelmistohäiriöt, virheet ja laiminlyönnit sekä tyytymättömät tai epärehelliset työntekijät.[20]

Tarkemmin uhat voidaan jakaa niiden tyypin mukaan esimerkiksi seuraavasti:[21]

1. Asiattomien pääsy systeemiin
2. Petos ja kavallus

---

[20] Saari, s. 164

[21] Garcia, s. 21 - 22

3. Toiminnan keskeytyminen tai toimintakyvyn heikentyminen
4. Inhimilliset erehdykset
5. Yksityisyyden loukkaus
6. Sabotaasi
7. Teollinen vakoilu
8. Muut uhat

Edellä mainitut uhat koskevat yleisesti ottaen kaiken kokoisia systeemejä. Tietojenkäsittelyn nopea kehitys ja tietojenkäsittelyn hajauttaminen ovat kuitenkin tuoneet mukanaan uusia uhkia ja varsinkin muuttaneet niiden luonnetta ja merkitystä. Suurimpina muutosten tuojina voidaan pitää henkilökohtaisten tietokoneiden määrän nopeaa kasvua, itsenäiskäytön lisääntymistä ja tehtävien monipuolistumista sekä tietoverkkojen lisääntymistä. Eräänä erityspiirteenä voidaan pitää ohjelmia, joiden tarkoituksena on, joko tuhota tai vahingoittaa tiedostoja tai joiden avulla yritetään hankkia laittomasti aineellista hyötyä.

Seuraavaksi käsitellään lyhyesti kutakin näistä uhkatekijöistä:

1. Asiattomien pääsy systeemiin

Keskitetyssä järjestelmässä asiattomien pääsyä systeemiin pystyttiin estämään pääosin valvomalla pääsyä keskustietokoneeseen ja tietojenkäsittelytiloihin. Ulkoisten yhteyksien puuttuminen sulki pois tätä kautta tapahtuvat tunkeutumisyritykset, jolloin systeemiin tunkeutuminen vaati pääsyä yrityksen tietojenkäsittelytiloihin. Normaalilla pääsyn- ja kulunvalvonnalla ja asiakastilojen erottamisella tietojenkäsittelytiloista päästiin suhteellisen helposti ja pienin kustannuksin riittävään turvallisuustasoon. Sensijaan hajautetussa järjestelmässä ei useinkaan ole mahdollista erottaa selkeästi asiakas- ja tietojenkäsittelytiloja, sillä tietokoneet ja oheislaitteet sijaitsevat fyysisesti hajallaan kaikkialla organisaatiossa. Samoin ulkoisia yhteyksiä tarvitaan yrityksen toiminnan tehostamiseksi eikä niiden karsiminen silloin ole tietojärjestelmän ja yrityksen toiminnan kannalta järkevää.

2. Petos ja kavallus

Hajautetussa järjestelmässä tietokoneet ja niiden käyttö yleistyvät kaikissa organisaation toiminnoissa ja sen eri tasoilla. Verrattuna keskitettyyn järjestelmään, jossa tietojenkäsittelyyn liittyviä tehtäviä hoiti suhteellisen pieni ja rajattu ryhmä, hajautetussa järjestelmässä yhä useammalla organisaation jäsenellä on mahdollisuus tietojärjestelmän väärinkäyttöön. Käytön valvonta ja käyttäjien hallinta vaati hajautetussa järjestelmässä selvästi enemmän panostusta kuin keskitetyssä järjestelmässä.

3. Toiminnan keskeytyminen tai toimintakyvyn heikentyminen

Hyvin suunniteltu ja toteutettu hajautettu järjestelmä ei ole yhtä altis fyysisille vahingoille kuin keskitetty järjestelmä. Yksittäiset mikrotietokoneet voidaan korvata suhteellisen nopeasti ja pienillä kustannuksilla, ja työtehtäviä voidaan siirtää helpommin työpisteestä toiseen. Riippuvuus verkon toiminnasta tai muista yhteyksistä voi aiheuttaa ongelmia, jos niitä ei ole huomioitu riittävän hyvin järjestelmän turvallisuussuunnitelmissa.

Tietojen saatavuus sekä niiden eheys ja luotettavuus vaikuttavat myös järjestelmän käytettävyyteen. Hajautetussa järjestelmässä tiedon käsittelyn ja tuottamisen tapahtuessa useissa eri paikoissa korostuu tiedonhallinnan ja tietojen suojaamisen merkitys järjestelmän toiminnalle. Samoin tietokantojen ylläpito ja hallinta tulee merkittäväksi osaksi tiedonhallintaa tietojärjestelmien toiminnan jatkuvuuden ja luotettavuuden kannalta.

4. Inhimilliset erehdykset

Inhimillisten erehdysten mahdollisuuteen vaikuttaa käyttäjien määrä ja heidän ohjelmien ja järjestelmän tuntemuksensa. Erehdyksiä voidaan rajoittaa ohjelmallisilla tarkistuksilla ja varmistuksilla sekä käyttäjien koulutuksella ja ohjestuksella.

5. Yksityisyyden loukkaus

Yksityisyyden loukkaukset liittyvät itsenäiskäytön lisääntymiseen ja tietojen saatavuuteen ja hallintaan. Tietojen salaisuusluokittelulla ja käyttäjien tietotarpeiden määrittelyllä voidaan rajata eri ryhmät siten, että kunkin henkilön tai ryhmän käytössä on vain heidän työssään tarvitsemansa tiedot ja ohjelmat. Elintärkeiden, luottamuksellisten tai muuten salaisiksi luokiteltujen tietojen käyttöä ja saatavuutta tulee valvoa erityisen tarkasti. Samoin niitä tuottavien tai käyttävien ohjelmien toimintaa tulee seurata. Myös tietosuojan kannalta eri lähteistä tulevien tietojen yhdistelyyn on syytä kiinnittää erityistä huomiota.

6. Sabotaasi

Sabotaasi tai tietojärjestelmän tahallinen vahingoittaminen tulee helpommaksi järjestelmän levitessä laajemmalle alueelle. Kuitenkin koko järjestelmän tuhoaminen tai toiminnan pysäyttäminen on hajautetussa järjestelmässä vaikeampaa kuin keskitetyssä, jossa keskuskoneen vioittaminen riitti järjestelmän pysäyttämiseen. Sen sijaan verkon yksittäisen solmukohdan tai verkkoon kytketyn mikrotietokoneen tai muun laitteen vahingoittamisen helppous riippuu lähinnä pääsyn ja kulunvalvonnan tehokkuudesta. Tietoliikenneverkkojen ja ulkoisten yhteyksien käytön lisääntyminen mahdollistaa sabotaasin myös organisaation ulkopuolelta. Esimerkiksi linjaliikenteen tukkeuttaminen, tietokoneeseen murtautuminen tai tietokonevirus saattavat aiheuttaa suurtakin vahinkoa yrityksen toiminnalle.

7. Teollinen vakoilu

Tietoverkkojen käyttö ja ulkoiset yhteydet lisäävät teollisen vakoilun mahdollisuutta, jos tätä ei ole huomioitu yhteyksien suunnittelussa ja käytössä. Sanomien salaus ja linjaliikenteen varmistaminen, samoin kuin pääsynvalvonta ovat eräitä tietoliikenteen turvallisuuteen vaikuttavia tekijöitä. Myös itsenäiskäytön lisääntyminen antaa yhä useammalle henkilölle mahdollisuuden päästä käsiksi arkaluontoisiin tai salaisiin tietoihin. Samoin yksin unohdettu

linjalla auki oleva mikrotietokone mahdollistaa esim. siivoojan tai korjausmiehen pääsyn käsiksi yrityksen tietoihin.

8. Muut uhat

Muihin uhkiin hajautetussa järjestelmässä voidaan lukea ohjelmat, joiden tarkoituksena on tuottaa vahinkoa järjestelmälle, sen ohjelmille ja tiedoille, lisääntyvä itsenäiskäyttö, tietoverkkojen käytön yleistyminen sekä mikrotietokoneiden erityispiirteet.

2.3.1 Mikrotietokoneet ja päätteet

Mikrotietokoneiden kaksi tyypillistä piirrettä, jotka tekevät ne samalla hyödyllisiksi, ovat paikalliset tietovarastot ja paikallinen tietojen käsittely. Samat piirteet kuitenkin luovat uhkatekijöitä mikrotietokoneiden käytössä.

Mikrossa oleva informaatio on paljon arkaluontoisempaa ja helpommin saatavilla kuin suurien monikäyttöjärjestelmien informaatio. Tietyssä koneessa oleva tieto liittyy yleensä yhteen henkilöön tai hyvin määriteltyyn ryhmään ja yleensä tieto on myös jalostetummassa tai lopullisessa muodossa. Tietoaineisto, joka normaalisti paperille tulostettuna viedään kassakaappiin, saatetaan esim. säilyttää levykkeellä hyllyssä. Varsinkin, jos mikrotietokoneessa on levykeasema tai modeemi, voidaan tietoa viedä tai tuoda tietokoneeseen ilman, että sitä olisi mahdollista kontrolloida. On epätodennäköistä, että yrityksissä tiedettäisiin tarkasti mitä tietoa yrityksen mikrotietokoneille on tallennettu.

Paikallisessa tietojen käsittelyssä eräänä ongelmana on laadun valvonta. Ammattiohjelmoijat noudattavat määrättyjä menetelmiä ja ohjeita ohjelmiensa laadun varmistamiseksi. Huolimatta virallisesta laadunvalvonnasta käyttäjät pyrkivät itse muuttamaan ohjelmia tai jopa tekemään niitä itse.[22] Muutokset

---

[22] Brown, 1989 s. 286

saattavat olla onnistuneitakin, mutta niistä ei dokumentoida, joka taas vaikeuttaa ohjelmien ylläpitoa ja eri ajojen tulosten vertailua. Muutokset saattavat myös aiheuttaa ohjelman tai tietojen tuhoutumisen tai vahingoittumisen.[23]

Mikrojen muita turvallisuuteen vaikuttavia piirteitä ovat mm. seuraavat:
- fyysinen luoksepäästävyys
- sisäänrakennetut turvallisuuspiirteet
- käyttäjät

Fyysisen luoksepäästävyyden kontrollointi mikroympäristössä on hyvin vaikeaa. Harvoin on järkevää yrittää rakentaa fyysistä suojaava "kuorta" mikron ympärille, ja siksi luvatonta fyysistä pääsyä on vaikea estää. Helppo luoksepäästävyys kuuluu olennaisesti käsitteeseen "henkilökohtainen" tietokone ja sen rajoittaminen samalla rajoittaisi helposti tietokoneen käyttömukavuutta.[24]

Useimmista mikroista puuttuvat sisäänrakennetut laitteistopiirteet, joita tarvittaisiin käyttäjien eristämiseksi arkaluontoisista, turvallisuuteen liittyvistä, systeemitoiminnoista, joilla luodaan tietokoneen sisäinen turvallisuus. Toisaalta voidaan yrittää suojata konetta ja tietoja esim. rajoittamalla käyttöoikeuksia erilaisilla ohjelmilla, mutta ohjelmiin perustuvat suojamekanismit voidaan ohittaa esim. käynnistämällä tietokone omalta levykkeeltä.[25]

Mikrojen turvallisuuteen ja suojattavuuteen vaikuttavia piirteitä ovat erityisesti levykkeet ja kiintolevyt sekä niille tallennetut tiedot ja ohjelmat, käyttäjäystävälliset systeemit, laitteiston vahinkoalttius, laadunvarmistus, dokumentointi, mikroympäristön tietoliikenneyhteydet ja laitteistojen yhteensopivuus.[26] Laitteistojen yhteensopivuus saattaa muodostua ongelmaksi ja turvariskiksi esimerkiksi silloin, kun yritetään laatia mikroympäristöön yleistä

---

[23] Ledell ym, s. 29

[24] Saari, s. 164

[25] Stephenson, 1989, s. 285

[26] Parker, 1988, s. 13

turvallisuusohjelmaa ja erimerkkisten laitteiden turvallisuuspiirteet eroavat toisistaan.

2.3.2
Itsenäiskäyttö

Henkilökohtaisten tietokoneiden turvallisuus riippuu suurimmalta osin sen käyttäjästä. Keskitetyssä tietojenkäsittelyssä tietojärjestelmien käyttöön ja turvallisuuteen liittyviä tehtäviä hoiti suhteellisen pieni, hyvinkoulutettu ryhmä. Käyttäjien koulutus ja käyttäjien vastuualueiden selventäminen on tärkeässä asemassa kehitettäessä henkilökohtaisen tietokoneen tietoturvallisuutta. Käyttäjien tulee noudattaa yrityksessä laadittuja turvallisuusohjeita ja -käytäntöjä ja heidän tulee ymmärtää vastuunsa tietojen, ohjelmien ja laitteistojen suojaamisessa.

Ongelmaksi saattaa muodostua myös varsinaisen käytön valvonta. Aikaisemmissa keskuskoneisiin pohjautuvissa järjestelmissä tällaiseen "omaan" käyttöön pystyivät lähinnä vain systeemisuunnittelija tai atk-päällikkö. Nykyisin, jos työntekijällä on käytössään henkilökohtainen tietokone, on vaikea löytää keinoja, joilla voitaisiin kontrolloida, mihin tietokonetta todellisuudessa käytetään.

2.3.3
Tietoverkot ja niiden suojaus

Tietoverkkojen yleistyminen ja niiden kasvava käyttö tiedon siirrossa tuo uusia uhkia sekä siirrettävän tiedon suojaukselle että yhteyksien toiminnan varmistamiselle väärinkäytösten ja virhetilanteiden yleistyessä. Yhteyksiä saatetaan vahingoittaa tahattomasti tai tarkoituksella, linjoja saatetaan kuunnella tai siirrettävää tietoa voidaan muuttaa tai vahingoittaa tai se saattaa kadota kokonaan. Samoin yrityksen toiminnalle kriittisten yhteyksien häiriöt tai katkeaminen vaikeuttaa yrityksen toimintaa ja saattavat jopa pysäyttää sen kokonaan.

Tietoverkkoja uhkaavat tekijät voidaan jakaa myös viiteen eri alueeseen: suunnitteluvirheet, katastrofit, tahalliset tai tahattomat tuottamukset, tietokoneen väärinkäyttö ja muut vaaratekijät.[27]

Suunnitteluvirheet aiheuttavat yleensä turhia ylläpito- ja korjauskustannuksia. Samoin ne voivat heikentää verkon toimintaa ja sen luotettavuutta.

Katastrofeihin voidaan lukea esimerkiksi tulipalo, vesi- tai muut nestevahingot, tuuli ja maanjäristykset, ja muut vastaavat tapahtumat joihin ei voida vaikuttaa, mutta joiden toteutumiseen voidaan varautua.

Tahallisiin tai tahattomiin tuottamuksiin kuulvat kaikki tietoverkkolaitteistolle, ohjelmistoille, verkkoon kuuluville tietokoneille ja tiedoille ihmisten tahallisesti tai tahattomasti aiheuttamat vahingot tai tuhot.

Tietokoneen väärinkäyttö tarkoittaa väärennettyjen viestien lähettämistä, viestien sieppaamista, lähetysten häirintää tai estämistä tai luvatonta tietoverkon tiedostoihin tunkeutumista.

Muihin vaaratekijöihin voidaan lukea tietoverkon laitteiston tai ohjelmien toimintavirheet, puutteellinen dokumentointi, riittämätön tietoverkon laitteiston tai ohjelmiston ylläpito, tietoverkon käyttäjien tai vastuuhenkilöiden puutteellinen koulutus, tietoverkon tiedostojen virheet tai tietojen puutteellinen eheys.[28]

Kansainvälisen standardointijärjestön tietoliikennestandardien (ISO/OSI) määrittelyn mukaisesti voidaan tietoliikenteen turvapalvelut jakaa viiteen eri osaan: [29]

---

[27] Jamieson & Low, 1989 s. 306

[28] Jamieson & Low, 1989, s. 308

[29] Salonen, s. 10

1. Tunnistus
-yhteyden tai keskustelun eri osapuolten on kyettävä yksiselitteisesti tunnistamaan toisensa

2. Pääsynvalvonta
-yhteyden saamiseksi on noudatettava ennaltamääriteltyä protokollaa, yhteyksiä ja yhteydenottoyrityksiä on valvottava

3. Tiedon luottamuksellisuus
-kuljetettavan informaation luottamuksellisuus ei saa vaarantua siirron aikana

4. Tiedon eheys
-informaatio ei saa muuttua, vahingoittua tai tuhoutua siirron aikana

5. Tiedon kiistämättömyys
-tiedon alkuperä ja oikeellisuus on pystyttävä kiistattomasti selvittämään

Turvapalveluiden toteuttaminen voidaan toisaalta jakaa karkeasti kolmeen osa-alueeseen:

- sovellukset suorittavat osapuolien tunnistuksen, tietosisällön salauksen, tiedon autenttisuuden ja eheyden varmistamisen

- kuljetuspalvelut suorittavat järjestelmätason tunnistukset, varmistavat siirron eheyden, tahdistuksen ja yhteyden palvelutasosta

- verkkopalvelut suorittavat liittymätason tunnistuksen, bittitason virheenkorjauksen ja huolehtivat verkon hallinnasta ja tarvittaessa linjasalauksesta. Sovelluspalvelut ja kuljetuspalvelut toimivat yleensä päästä päähän käyttäjien sovellusten ja laitteiden välillä, eivätkä yleiset televerkon järjestelmät puutu niiden toteutukseen.

Tietoverkkojen suojauksessa voidaan uhkatekijät jakaa myös sen mukaan tulevatko ne järjestelmän ulkopuolelta vai järjestelmän sisäpuolelta. Sisäiset uhat muodostuvat lähinnä järjestelmän käyttäjien ja yrityksen tietojärjestelmän ominaispiirteiden aiheuttamista riskeistä ja ulkoiset uhkatekijät johtuvat yrityksen ulkoisista yhteyksistä.

Sisäisiä uhkia voidaan rajoittaa sekä laiteratkaisuilla että ohjelmallisesti. Nykyisin on tarjolla suhteellisen runsaasti erilaisia turvaohjelmia, joilla voidaan rajoittaa käyttäjien valtuuksia koneen käytössä. Esimerkiksi lähiverkon käyttäjille on mahdollista luoda useita tarkistus- ja rajoitustasoja; systeemiin sisäänkirjoittautuessa vaaditaan käyttäjätunnus ja salasana, käyttäjälle määritellään tiedostot, joita hän saa käyttää sekä tiedostojen sisällä käyttäjäkohtaisesti määritellyt oikeudet (tiedon luku-, kirjoitus-, muutos-, tuhoamis- yms. oikeudet). Lisäksi tiedostoja on mahdollista piilottaa tai tiedot voidaan tallentaa salakirjoitettuina.

Helpoin tapa varastaa tietoa on tallentaa se työaseman kautta levykkeelle. Eräät yritykset ovat yrittäneet vähentää sisäisiä tietovuotoja ottamalla käyttöön sellaisia lähiverkon työasemia, joissa ei ole levykeasemia.[30] Toinen tapa on käyttää erikoislevykkeitä, jotka saavat aikaan hälytyksen, jos niitä yritetään viedä pois yrityksen tiloista.[31]

Ulkoapäin tulevia uhkia pystytään parhaiten torjumaan karsimalla ulkopuolisia yhteyksiä ja valitsemalla mahdollisimman turvalliset linjat. Itse suunnitellut ja rakennetut linjayhteydet ovat aina turvallisempia kuin yleiset linjat tai puhelinverkot. Omiin yhteyskaapeleihin on esimerkiksi mahdollista asentaa elektroninen tunnistin, joka hälyttää mikäli niihin yritetään kiinnittyä.[32] Yleisiä suojatoimia ovat myös käyttäjän tunnistus sekä sanomien salakirjoitus. Käyttäjän tunnistukseen voidaan käyttää tunnussanaa tai biometrisiä laitteita

---

[30] Brown, 1989, s. 286

[31] Zajac, 1988, s. 249

[32] Jamieson & Low, 1989, s.316

kuten sormenjälkien, kädenmuodon, äänen, verkkokalvon tai elektronisen nimikirjoituksen tunnistus. Mikäli tunnistus halutaan varmistaa, voidaan tunnistamiseen käyttää useita eri menetelmiä samanaikaisesti, pelkkä tietämyspohjainen tunnistus ei riitä. Tällöin tunnistus voi perustua

A) omistukseen (tunnistuskortti),

B) tietämykseen (salasana) ja

C) luonteenpiirteeseen (elektroninen allekirjoitus).

Yhteydenottoprotokollan tulisi sisältää ainakin sen, että yhteyden saaminen perustuu käyttäjän tunnistukseen ja salasanan tarkistamiseen, terminaaliyhteydet tulisi katkaista määräajan jälkeen mikäli niitä ei käytetä ja yhteys tulisi katkaista esim. kolmen epäonnistuneen tunnistuksen jälkeen.[33] Sanomien salaamiseen on tarjolla myös useita laite- ja ohjelmaratkaisuja, jotka poikkeavat toisistaan lähinnä salaustekniikan ja avainten käsittelyn kannalta.

Tiedonsiirtoverkon toimivuuden seuraamiseksi ja parantamiseksi tulisi luoda verkon valvontajärjestelmä. Valvontajärjestelmän tehtävänä on tuottaa selkeää tietoa verkon eri tapahtumista; tiedonsiirron määristä, virheistä ja häiriöistä. Järjestelmän täytyy myös kyetä reagoimaan ulkopuolisten aiheuttamiin häiriöihin ja tunkeutumisyrityksiin. Erilaisia lokitiedostoja käyttämällä voidaan valvoa järjestelmän käyttöä ja yhteyksiä. Valvonnan on oltava jatkuvaa ja seurantatiedon helposti ymmärrettävää ja käsiteltävää.

Yrityksen tiedonsiirtoyhteyksien varassa toimiville toimipisteille on tärkeää, että tarvittava tieto on aina saatavilla. Häiriöttömän toiminnan varmistamiseksi fyysisiä uhkia vastaan (kaapelivauriot, puhelinkeskusten häiriöt tms.) yhteys voidaan varmistaa esim. kahdentamalla se tai suunnittelemalla varajärjestelmä, jota kautta tarvittavat tiedot voidaan siirtää. Täysin hajautetussa järjestelmässä voidaan työpisteet suunnitella siten, että tarvittaessa tehtäviä voidaan

---

[33] Highland, 1989, s. 553

saumattomasti siirtää toiselle työpisteelle. Tällainen järjestelmä voidaan ajatella eri itsenäisten toimintamodulien muodostamaksi hajautetuksi kokonaisjärjestelmäksi. Modulien ja niiden toiminnan on oltava korvattavissa toisilla järjestelmän moduleilla ja yhden tai useamman modulin toiminnan keskeytymisen vaikutus muihin moduleihin ja koko järjestelmän toimintaan on minimoitava. Tällaisen modulaarisen järjestelmän pohjana voidaan käyttää esim. yrityksen eri toimintaprosesseja, jolloin järjestelmän osat muodostuisivat yrityksen toimintojen perusteella.

2.3.4
Väärinkäytökset ja rikokset

Viime aikoina paljon julkisuutta ovat saaneet ns. tietokonevirukset, jotka pystyvät monistautumaan; kopioimaan ja kiinnittämään osia itsestään muihin ohjelmiin. Osa viruksista on "hyvänlaatuisia", ne eivät tuhoa tiedostoja, mutta kopioituvat silti ohjelmiin ja kuluttavat näin tietokoneresursseja. Toiset virusohjelmat ovat haitallisempia, ne tuhoavat tehokkaasti ohjelmia ja tietoja ja pahimmillaan ne tuhoavat tietokoneen kaikki tiedostot ja estävät koko koneen toiminnan.

Yhdysvalloissa ja muualla Euroopassa virusuhkaan on tähän asti kiinnitetty enemmän huomiota kuin Suomessa. Maailmassa on kaiken kaikkiaan todettu noin 5000 erilaista virusta, mutta Suomi on pysynyt syrjäisen sijaintinsa ansiosta suhteellisen pitkään vapaana niistä. Ehkä juuri siksi niihin ei Suomessa ole kaikilla tahoilla suhtauduttu riittävän vakavasti. Viime aikoina viruskanta on kuitenkin kasvanut myös Suomessa, ja virushavainnot eri puolilla Suomea ovat lisääntyneet, samoin niiden aiheuttamat tuhot. Suuri osa viruksista löydetään eri oppilaitosten tietokoneista, mutta viruksia on alkanut löytyä yhä enemmän myös yrityksien tietokoneista sekä yksityisten ihmisten kotikoneilta.

On olemassa myös muita viruksen tyyppisiä ohjelmia, esimerkiksi ns. matoja. Mato on itsenäisesti toimiva ohjelma, joka pyrkii leviämään toisiin järjestelmiin. Eräänä esimerkkinä Yhdysvalloissa sai vuonna 1988 suurta julkisuutta ns. Morrisin mato, joka pääsi leviämään Yhdysvaltojen ilmavoimien

tietokonejärjestelmiin, sekä erääseen ydinaseiden suunnitteluun käytettävään järjestelmään.[34]

Muita vahingollisia ohjelmatyyppejä ovat mm. "Troijan Hevonen" (the Trojan Horse); ohjelma, joka tekee todellisuudessa jotain muuta kuin miltä sen toiminta ulospäin näyttää, "Looginen pommi" (the Logic Bomb) tai "Aikapommi" (the Time Bomb); ohjelma, joka määrittelee ajankohdan tai olosuhteet, milloin ohjelma käynnistyy, tuhoten tietokoneen tiedostot tai estäen sen toiminnan.[35]

"Salami" (the Salami), on pieni ohjelma, joka tekee pääohjelmaan tai sen ajotuloksiin pieniä muutoksia jokaisella ajokerralla. Esimerkiksi pankkijärjestelmässä voidaan tuhansilta tileiltä ottaa pennejä jokaisesta tapahtumasta itse hallitsemalleen tilille, josta rahat voidaan myöhemmin nostaa. Siirrettävät summat ovat niin pieniä, etteivät asiakkaat huomaa menettäneensä mitään.

2.3.5
Fyysinen ja laitteiston suojaus

Hajautettu tietojärjestelmä, laajalle alueelle jaettuine laitteistoineen, ei ole yhtä haavoittuva esimerkiksi sähköhäiriöille, luonnontuhoille ja hyökkäyksille kuin keskitetty järjestelmä.[36] Hajautetussa järjestelmässä on epätodennäköisempää, että koko järjestelmä tuhoutuu. Toimintojen hajauttaminen on kuitenkin moninkertaistanut yksittäisiin mikrotietokoneisiin varastoidun tiedon määrän ja arvon, jolloin yhdenkin henkilökohtaisen tietokoneen sisältämän tiedon tuhoutuminen saattaa aiheuttaa yritykselle suurta vahinkoa. Samoin laitteisto on kokonsa ja painonsa vuoksi helposti siirrettävissä ja varastettavissa. Siksi laitteistoa ei pitäisi säilyttää kovin näkyvillä paikoilla ja niiden luoksepäästävyyttä olisi mahdollisuuksien mukaan rajoitettava.[37]

---

[34] HS 05.03.90, s. 7

[35] Adney & Kavanagh, 1989, s. 267

[36] Moulton, 1983, s. 124

[37] Grimson & Kugler, s. 298

2.3.6
Tiedon suojaus

Tärkeimpiä tiedon turvaamistoimia ovat selvien toimintaohjeiden laatiminen ohjelmien ja sovellusten normaalikäyttöön sekä selvien ennalleenpalautusohjeiden laatiminen. Erittäin tärkeää on varmuuskopiointi ja kopioiden säilyttäminen turvallisessa paikassa. Keskitetyssä tietojärjestelmässä varmuuskopiointi on yhden tai useamman ennaltamäärätyn atk-koulutetun henkilön tehtävänä ja varmuuskopiointi suoritetaan keskitetysti ja säännöllisesti. Hajautetussa järjestelmässä kukin henkilökohtaisen tietokoneen käyttäjä itse on yleensä vastuussa varmuuskopioinnista ja niiden säilyttämisestä. Hajautetussa järjestelmässä yrityksen on huolehdittava siitä, että vastuu ja tehtävät ovat selkeästi määritelty, ja että käyttäjien koulutus on riittävällä tasolla.

Koulutuksen tulisi kattaa kaikki ne henkilöt, joilla on kosketus tietojärjestelmään. Hajautettuun tietojenkäsittelyyn kuuluvat suojatoimien erityispiirteet on selvitettävä käyttäjille. Peruskoulutuksen tavoitteena on saada käyttäjät ymmärtämään turvajärjestelyjen tarpeellisuus ja saada käyttäjät suhtautumaan niihin myönteisesti. Tuloksena saadaan turvajärjestelyjen tarkempi noudattaminen ja turvajärjestelmien parempi käyttö.

Monet yritykset ovat nykyisin kieltäneet ulkopuolisten ohjelmien, esim. pelien, asentamisen yrityksen tietokoneisiin ja samalla ohjelmien hankinta suoritetaan keskitetysti tai tiettyjen ohjeiden ja suositusten perusteella.[38] Tällä tavoin pyritään estämään virusohjelmien leviämistä ja ohjelmien laadunvalvonta helpottuu.

Uusimmissa tietokoneissa on usein mahdollista lukita näppäimistö, jolla estetään satunnaista ohikulkijaa kirjoittamasta "format" tai "del *.*", joilla

---

[38] Zajac, 1988, s. 250

voidaan tuohota tiedostoja, mutta jos on kyse verkkoon kytketyistä koneista, ei lukituksesta ole hyötyä elleivät kaikki koneet ole suojattu samalla tavalla.

2.3.7
Katastrofi- ja toipumissuunnitelmat

Katastrofisuunnitelman avulla on tarkoitus varautua etukäteen erilaisiin toiminnan häiriöihin. Suunnitelmassa sovitaan etukäteen milloin katastrofisuunnitelmaa aletaan soveltaa, mitä tehdään ja ketkä ovat vastuussa siitä, että suunnitelmaa noudatetaan. Lopuksi pyritään palauttamaan normaalit toiminnot mahdollisimman nopeasti ja mahdollisimman vähäisin kustannuksin.

Katastrofisuunnitelman tulee kattaa laitteiston, ohjelmien ja tietojen sekä toimintojen ja palvelujen elvyttäminen. Siksi katastrofisuunnitelman toimiminen riippuu muiden tietoturvan kohteiden kuten tiedostojen varmuuskopioinnin ja fyysisen suojauksen toteuttamisesta. Koska katastrofin jälkeinen toimintojen elvyttäminen saattaa tarkoittaa varajärjestelmään siirtymistä ja toiminnan suurta sopeuttamista toipumisen aikana, on suunnitelmaa testattava ja sen toimintaa harjoiteltava ainakin tärkeimpien sovellusten osalta.[39]

3
ATK-RISKIT

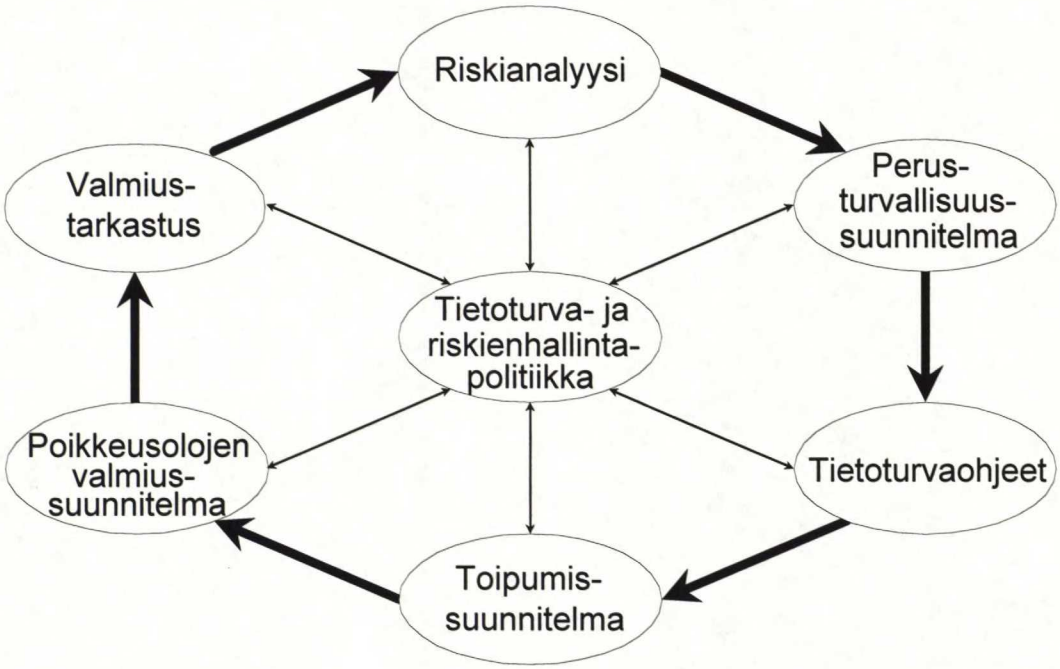
Yrityksen informaatiosysteemien strategian määrittelyyn ei nykyisin riitä perinteinen kustannus- ja hyötyajattelu. Pitkälle hajautettu tietojenkäsittely, monimutkaiset tietoverkot ja tietokantasysteemit ovat tehneet riskistä kolmannen tekijän informaatiosysteemien suunnittelussa.[40]

---

[39] Tietosuojan toteuttamisohjeet, s. 21

[40] Tate, 1988, s. 58

Kuvio 5 Riskienhallinnan pelikenttä



Laite- ja muun ympäristön, tiedon ja tietoverkkojen turvallisuusnäkökohtien lisäksi on otettava laajalti huomioon myös muita yrityksen toimintaan vaikuttavia seikkoja, kuten tietovirrat, tietojen eheys ja volyymi. Niissä esiintyvistä puutteista seuraa myös organisaation heikkoudet; puutteellinen johtamiskyky ja toisistaan riippuvaiset systeemit. Perinteiseen atk-turvallisuuteen perustuvat toimenpiteet ovat suhteellisen passiivisia ja keskitetyn järjestelmän turvallisuusongelmat ovat melko staattisia; nykyisin kuitenkin järjestelmän haavoittuvuus aiheutuu usein teknologian, sovellusalueiden ja informaatiojärjestelmien jatkuvasta muutoksesta.[41]

Tietojärjestelmien haavoittuvuuden kasvaessa on tietojärjestelmien riskienhallinnassa yhä yleisemmin otettu käyttöön riskien arviointi- ja riskianalyysimenetelmiä, joita käytetään tietojärjestelmien turvallisuuden arvioinnin työkaluina. Näiden työkalujen käytön perimmäisenä tarkoituksena on auttaa tietojärjestelmien omistajia ja käyttäjiä ymmärtämään kohtaamiensa riskien luonne ja laajuus. Samalla riskianalyysin avulla saatetaan liiketoiminnan

[41] Tate, 1988, s. 64

kannalta merkittävät riskit yritysjohdon tietoisuuteen ja pyritään antamaan riittävästi tietoa tietoturvaan liittyvää päätöksentekoa varten.

3.1
Atk-riskien hallinta

Atk-riskien hallinta on kokonaisnäkemys olemassa olevista järjestelmää uhkaavista vaaroista ja järjestelmällinen tutkimus siitä, miten niistä aiheutuvat menetykset voidaan minimoida sekä tähän tutkimukseen perustuva edullisimpien hallintakeinojen valitseminen ja toteuttaminen. Organisaation ja tietohallinnon johdon tulisi tiedostaa atk-järjestelmää ympäröivät riskit ja pystyä arvioimaan niiden todennäköisyys ja suuruus sekä minimoida tunnistetusta riskeistä yritykselle aiheutuvat menetykset ja sitä kautta turvata tietojärjestelmän ja koko yrityksen toiminnan jatkuvuus.

Riskien alkuperäiset syyt ovat usein tavoittamattomissa ja varsinkin suurempiin järjestelmiin sisältyy niin paljon mahdollisia uhkia, että niiden täydelliseen eliminoimiseen tarvittaisiin valtava määrä resursseja. Onkin huomattava, että vaikka riskejä voidaan rajoittaa tai kontrolloida, niitä ei pystytä kokonaan eliminoimaan[42].

Päätöksentekijän ei siis kannata pyrkiä riskien eliminoimiseen vaan niiden hallintaan. Käytännössä tämä edellyttää niiden erityyppisten riskien luonteen ja laajuuden ymmärtämistä, joiden kohteeksi järjestelmä voi joutua. Samoin on määriteltävä, minkätasoinen riski on katsottava hyväksyttäväksi siinä ympäristössä missä järjestelmä toimii, ja minkä verran resursseja kannattaa uhrata joko riskin aiheuttamina vahinkoina tai turvallisuuskontrollien ja turvatoimien soveltamisena. Soveltamalla ja ottamalla käyttöön asianmukaisia ja kustannuksiinsa nähden tehokkaita kontrolleja voidaan alentaa

---

[42] Saari, 1989, s. 238

olemassaolevat riskit tasolle, jota voidaan analyysin perusteella pitää hyväksyttävänä.[43]

Organisaation näkökulmasta riskien hallinta prosessina voidaan jakaa neljään eri vaiheeseen:[44]

1. Riskien tunnistaminen
2. Riskien arvioiminen
3. Riskien hallintatoimista päättäminen
4. Valittujen hallintatoimien toteutus

Riskien tunnistamiseen voivat osallistua kaikki yrityksen työntekijät. Mikäli mahdollista, riskin havaitsija luonnollisesti poistaa tai yrittää pienentää riskiä. Riskien tunnistamiseen voidaan käyttää myös riskikartoitusta tai asiantuntijan apua.

Riskien arvioinnilla tarkoitetaan nykyisin niitä analyyttisiä toimenpiteitä, joiden avulla systeemiin mahdollisesti vaikuttavien uhkien luonnetta ja seurausten laajuutta tutkitaan ja arvioidaan. Tietojenkäsittelyn riskien arvioiminen vaati usein atk:n tuntemusta ja siksi se on tehtävä atk-asiantuntijoiden ja käyttäjien yhteistyönä.

Riskien hallintatoimista päätettäessä on useita eri vaihtoehtoja: riskin välttäminen, riskin poistaminen, riskin pienentäminen, riskin siirtäminen tai riskin pitäminen itsellään. Eri toimintatapoja vertailtaessa on taloudellisilla tekijöillä suuri merkitys ja usein on edullisinta yhdistää useita eri hallintakeinoja.

Valittujen hallintatoimien toteutus jää asianosaisille organisaation osille toimeenpantavaksi. Toteutukseen kuulu myös käyttöönottovaiheen valvonta ja jälkiseuranta, mikäli toimenpiteet monimutkaistavat järjestelmää. Usein on

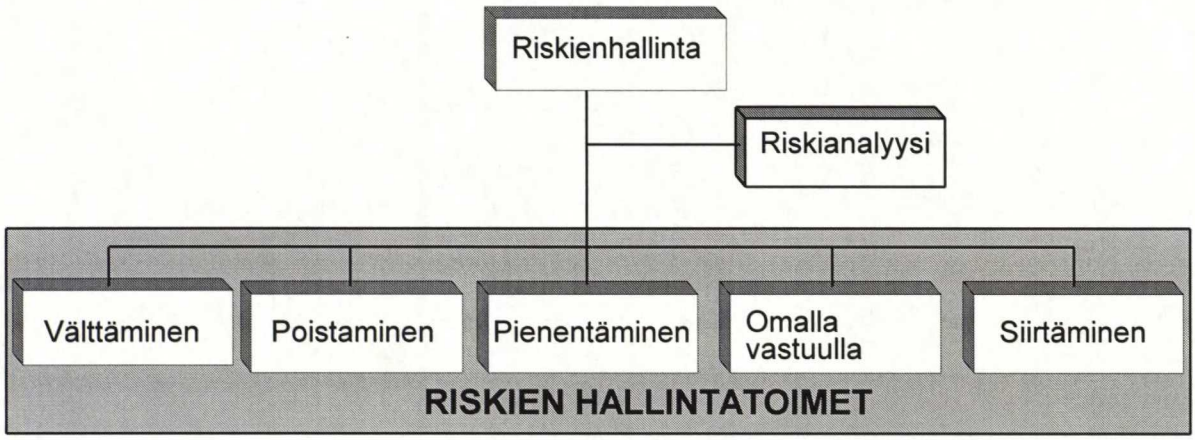
---

[43] Saari, 1989, s. 238

[44] Kainomaa, s. 5

havaittu, että hyväkin varmuustoimenpide jää käytännössä suorittamatta, jos muutokset lisäävät jonkin toiminnon työmäärää tai lopullinen suorittaja ei ymmärrä sen tärkeyttä.[45]

Kuvio 6 Atk-riskien hallinnan toimenpiteet



Lähde: Juha Ettala, Riskienhallintastrategia 1986

3.2
Atk-riskien arviointi ja analysointi

Riski määritellään ei-toivotun tapahtuman todennäköisyydeksi ja se voidaan esittää matemaattisesti riskitulona, jonka muodostavat riskin toteutumisen todennäköisyys ja tapahtumasta seuraavat kustannukset.

Riskitulo:

Riski = ei-toivotun tapahtuman esiintymistodennäköisyys X ei-toivotun tapahtuman kustannukset

Järjestelmän riskitaso on kaikkien riskien riskitulojen summa, jota ennalta määritellyn turvallisuustason saavuttamiseksi pyritään alentamaan vahingontorjunta- ja suojelutoimenpiteillä. Tietojärjestelmää tarkasteltaessa

[45] Kainomaa, s. 6 - 7

riskit ovat vahinkoriskejä, ja ne poikkeavat yrityksen normaaleista liikeriskeistä siinä, että vahinkoriskeistä puuttuu liikeriskeille ominainen voiton mahdollisuus. Vahinkoriskiin liittyy ainoastaan taloudellisen tai muun menetyksen mahdollisuus. Atk-riskejä voidaan nimittää myös tietoriskeiksi, jolloin tarkoitetaan vahingonvaaraa, joka kohdistuu automaattisen tietojenkäsittelyjärjestelmän kautta yrityksen hallussa olevaan tietoon, toimintaan, henkilöstöön, käyttöomaisuuteen tai varallisuuteen. Tietoriskin toteutuminen voi merkitä yritykselle huomattavia taloudellisia menetyksiä, toiminnan vaikeutumista, vahingonkorvausvelvollisuutta ja jopa asiakassuhteiden ja yrityskuvan vaurioitumista.46

Atk-riskejä analysoimisessa voidaan riskit luokitella esim. järjestelmälle sallittujen keskeytysten kestoaikojen mukaan. Luokitus voidaan tehdä toteutuneiden riskien aiheuttamien häiriöiden tai katkosten keston vaikutuksesta järjestelmän toimintaan. Selvitys tehdään koko järjestelmän kannalta sekä huomioiden erityisesti organisaation kriittiset toiminnot. Selvityksen perusteella voidaan määritellä järjestelmän häiriöiden sietokyky. Häiriöiden sietokyvyn mukaan toiminnot ja järjestelmä voidaan luokitella esim. seuraavasti:

1. järjestelmä ei siedä häiriöitä /katkoksia
2. 5 - 30 min katkos siedettävä
3. enintään 1/2 vrk:n katkos siedettävä
4. 1 - 3 vrk:n katkos siedettävä
5. useiden vuorokausien / viikkojen katkos siedettävä

Kukin järjestelmän toiminto arvioidaan ja toiminnot asetetaan järjestykseen niiden kriittisyyden perusteella. Riskeistä saadaan taloudellinen projisio arvioimalla riskin toteutumisen, toiminnan keskeytyksen tai alentuneen toimintatehon ja varajärjestelyjen organisaatiolle aiheuttamat kustannukset. Näitä kustannuksia voidaan pitää vertailulukuna suunniteltaessa järjestelmän toimintaa turvaavia toimenpiteitä.

---

46 Pohjola s.37

3.3
Atk-riskien hallinnan kustannukset

Yrityksen tulee myös tietoturvallisuudessa pyrkiä samaan kustannustehokkuuteen kuin muissa toiminnoissaan. Suurillakaan suojauskustannuksilla ei voida taata täydellistä turvallisuutta, mutta toisaalta, jos suojaustoimenpiteet eivät ole tarpeeksi kattavat, alkavat vahingoista aiheutuvat mentykset kasvaa nopeammin kuin mitä suojaustoimien karsimisella säästetään.[47] Perussääntönä suojaustoimien mitoittamisessa on se, että kustannukset eivät saa ylittää suojattavien tietojen, laitteiden tai resurssien arvoa.[48]

Ongelmallista riskien kustannusten arvioinnissa on järjestelmän ja sen sisältämän tiedon, organisaation informaatio-omaisuuden, arvon määrittäminen. Suoraan organisaation toiminnan tehokkuuteen vaikuttavien riskien toteutuminen tai fyysisten vahinkojen aiheuttamat kustannukset on helpompi arvioida kuin tieto-omaisuuteen tai muihin "näkymättömiin arvoihin" kohdistuvia vahinkoja . Lähtökohtana voidaan käyttää informaation uudelleenhankintakustannuksia ja sen vaatimia työmääriä. Kuitenkin esim. menetettyjen mahdollisten asiakkaiden tai yrityskuvan heikkenemisen rahallinen arviointi on erittäin vaikeaa. Yleensä on tyydyttävä pelkkään arvioon.

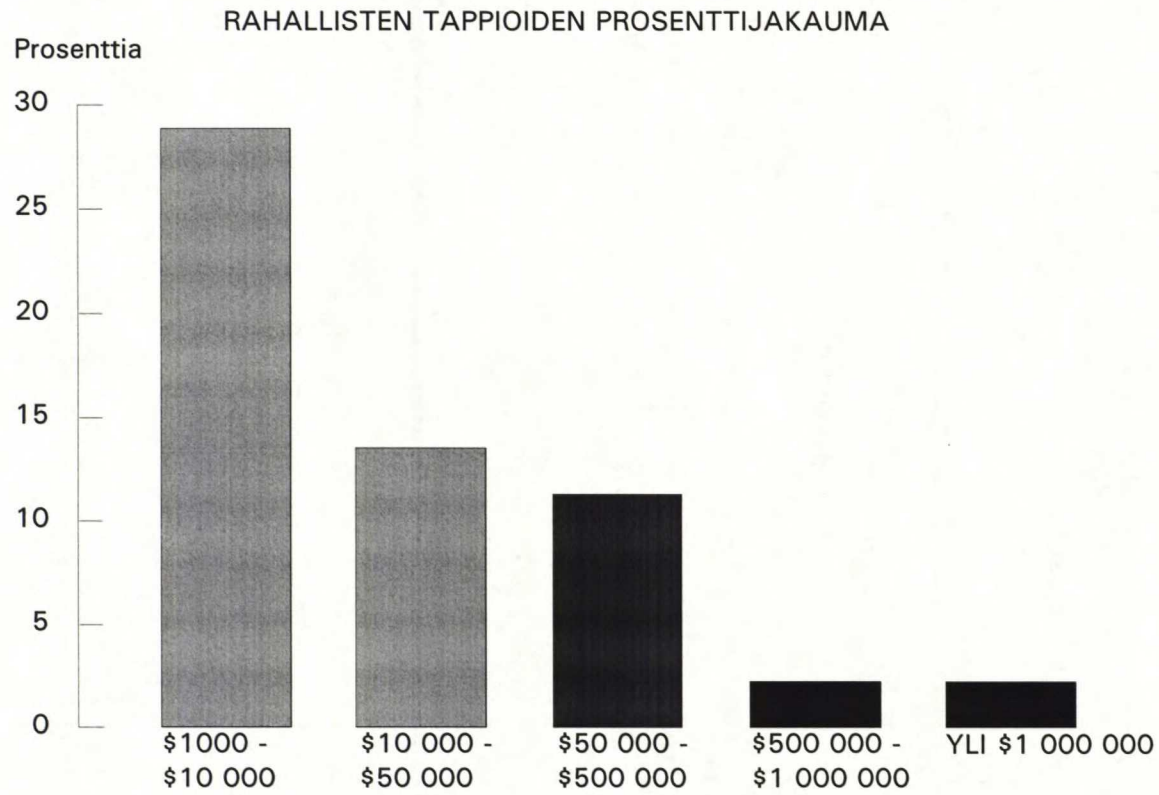
Vahinkojen rahallinen arviointi on ongelmallisuudestaan huolimatta kuitenkin tärkeää halutun tietoturvatason määrittämisessä. Samoin perustelut tietoturvan vaatimien resurssien ja panosten hankkimiselle edellyttävät yleensä kustannusarviota, jolloin on voitava esittää tietoturvainvestointien tuotot (= säästetyt vahinkomenot).

---

[47] Kainomaa, s. 7

[48] Booth, s. 280

Kuvio 7 Tietoturvavahinkojen aiheuttamat rahalliset tappiot



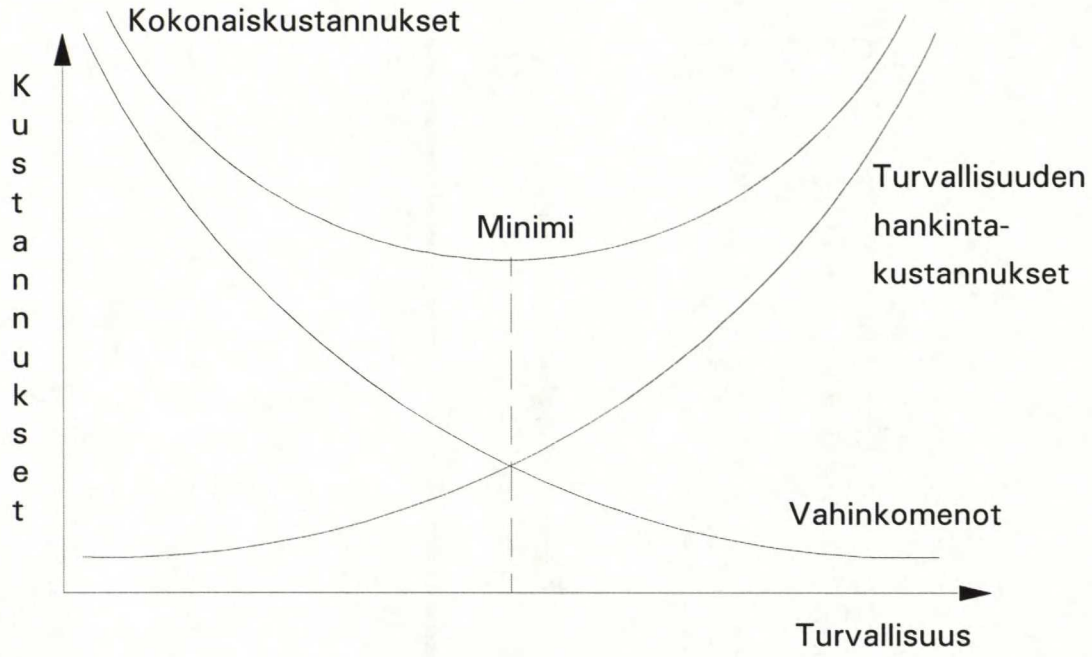
Lähde: Ernst And Whinney, U.S. Computer Security Surve 1987

Kuviossa 15 on esitetty erään tutkimuksen mukaan tietoturvavahinkojen aiheuttamien rahallisten tappioiden prosentuaalinen jakauma.

Tutkimuksen tietoihin tulee kuitenkin suhtautua varauksella ja pitää niitä lähinnä suuntaa antavana, sillä tietoturvavahinkojen arviointi on vaikeaa ja voidaan olettaa, että suurin osa vahingoista ei tule julkisuuteen.

Riskien hallintatoimilla pyritään siis minimoimaan vahingosta aiheutuvien kustannusten ja suojautumiskustannusten summa. Tietoturvallisuus- ja kustannustason määräytyminen on esitetty kuviossa 16. Sen mukaisesti tietoturvallisuustason optimi on samassa kohdassa kuin kokonaiskustannusten minimi.

Kuvio 8 Tietoturvallisuustason ja kustannustason määräytyminen



Lähde: Wong, s. 130

Riskinhallintaa voidaan siis kutsua menetelmäksi, jolla pyritään saavuttamaan yritykselle määritelty tietoturvallisuustaso minimoimalla toteutuneiden riskien ja uhkien aiheuttamat vahinkokustannukset optimoimalla vahinkomenojen ja turvallisuuskustannusten summa.

4
TIETOTURVAN KEHITTÄMISSUUNNITELMA

Tietoturvan päätehtävä on organisaation toiminnan kannalta elintärkeiden atk-järjestelmien ja tietoliikenneyhteyksien suojaaminen. Tietoturvalla pyritään varmistamaan atk-palvelujen ja -materiaalin saatavuus häiriöistä ja poikkeusoloista riippumatta sekä ennaltaehkäisemään vahinkojen tapahtumista. Tämä voidaan taata ainoastaan ennalta määritellyllä ja suunnitelmallisella toiminnalla toiminnan ja tietojärjestelmien turvaamiseksi. Tietoturvan kehittäminen lähtee liikkeelle tietoturvaan vaikuttavien eri tekijöiden analysoinnista. Riskianalyysissä määritellyt uhat ovat pohjatietoina tietoturvan kehittämissuunnitelman eri osa-alueilla, jonka tavoitteet taas määritetään organisaation tietoturvapolitiikassa.

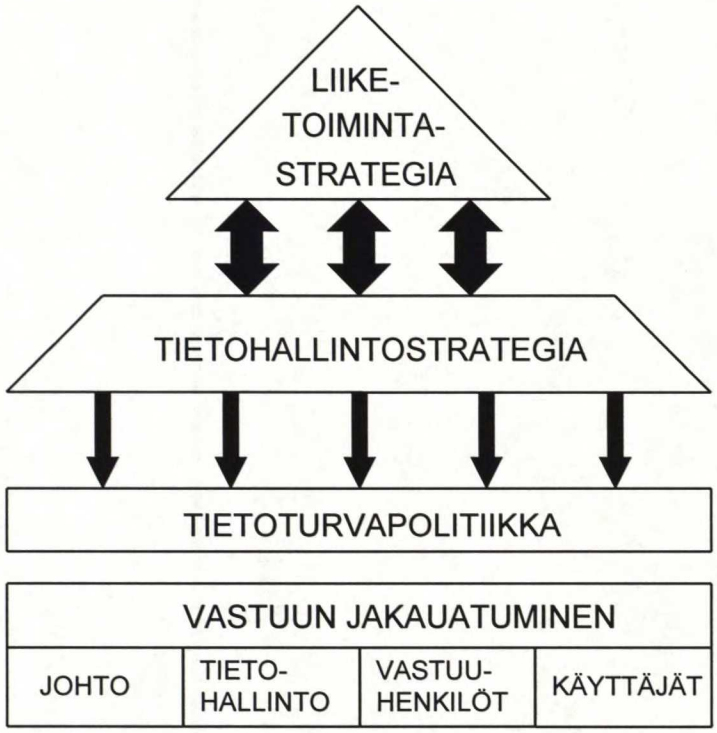
Tietoturvan kehittäminen ei ole kertaluontoinen tapahtuma, vaan se on prosessi, jota on vietävä eteenpäin kaiken aikaa. Organisaation ja sen toiminnan sekä ympäristön muutokset vaikuttavat koko ajan tietoturvalle asetettuihin vaatimuksiin. Samoin jokaisen eri osa-alueen sisällä tapahtuu jatkuvasti muutoksia, joita on tarkasteltava myös tietoturvan kannalta. Osa toimenpiteistä ja määritelmistä pysyy suhteellisen staattisina muutoksista huolimatta, osa saattaa muuttua hyvinkin radikaalisti, jolloin suunnitelmien päivittäminen ja iterointi on suunnitelman toimivuuden kannalta erittäin tärkeää.

4.1 Organisaation tietoturvapolitiikka

Tietoturvapolitiikan tulisi olla osa organisaation tietojenkäsittelyn strategiaa ja pohjautua näin ollen liiketoiminta- ja tietohallintostrategioiden määrittelyyn. Sen tehtävänä on suojata organisaatio tietojärjestelmää uhkaavilta riskeiltä ja varmistaa toiminnan jatkuvuus kriisitilanteissa. Vastuu tietoturvapolitiikasta on organisaation johdolla, tulosyksiköiden johdolla ja toimintojen esimiehillä omalla alueellaan. Tietoturvapolitiikan tulisi kattaa tietojärjestelmän käyttö, suojaaminen ja toiminnan turvaaminen. Tietoturvapolitiikka määrittelee organisaation suhteen tietoturvallisuuteen, ottaa kantaa tietojärjestelmän ja sen toiminnan merkityksen organisaatiolle sekä päättää halutusta tietoturvatasosta ja siihen uhrattavista resursseista. Tietoturvapolitiikan pohjalta organisaation atk-toiminnasta vastaava osasto ja nimetyt vastuuhenkilöt voivat päättää tarvittavista toimenpiteistä ja tietoturvan toteutuksen koordinoinnista, mutta vastuu pysyy kuitenkin johdolla, tulosvastuullisilla esimiehillä ja järjestelmien omistajilla.

Organisaation tietoturvapolitiikan tulee olla selvillä kaikilla eri organisaation tasoilla. Tietoturvapolitiikan pohjalta laaditut tietoturvaohjeet ja -säännöt on jaettava kirjallisina kaikille tietojärjestelmää käyttäville. Vastuu tietoturvallisuudesta jakaantuu johdon, atk-johdon, omistajien ja vastuuhenkilöiden ja atk-palvelujen käyttäjien kesken.

Kuvio 9 Tietoturvan kehittämisen toimintakehys



Johto on tietoturvapolitiikan kautta vastuussa tietojärjestelmän ja informaatio-omaisuuden suojaamisesta. Sen tulee järjestää alaisilleen riittävä koulutus ja varmistua siitä, että alaiset ovat tietoisia tietoturvapolitiikasta. Johdon tehtäviin kuuluu myös turvallisuuskontrollien noudattamisen valvonta.

Atk-johto on vastuussa yleisestä tietoturvallisuudesta koko järjestelmän kannalta. Erityistehtävinä voidaan mainita turvallisuuskäytäntöjen, ohjeiden ja menetelmien kehittäminen ja turvallisuutta parantavien toimenpiteiden suosittaminen sekä käyttäjien ja atk-informaation omistajien tuki. Atk-johdolla tulee olla hyvä näkemys järjestelmän riskeistä ja niiden välittömistä vaikutuksista toimintaan. Samoin atk-riskien selvittäminen yleisjohdolle kuulu lähinnä atk-johdon tehtäviin.

Informaation omistajaksi voidaan nimetä se toiminto, joka tuottaa tai käsittelee kyseistä tietoa. Omistajat voidaan määritellä myös esim. osastoittain tai vastuualueittain. Heidän tehtävänään on luokitella atk-informaatio ja määritellä kullekin luokalle riittävä turvallisuustaso ja tarvittavat kontrollit. Samoin he

huolehtivat omalla vastuualueellaan tietoturvapolitiikan ja ohjeiden noudattamisesta.

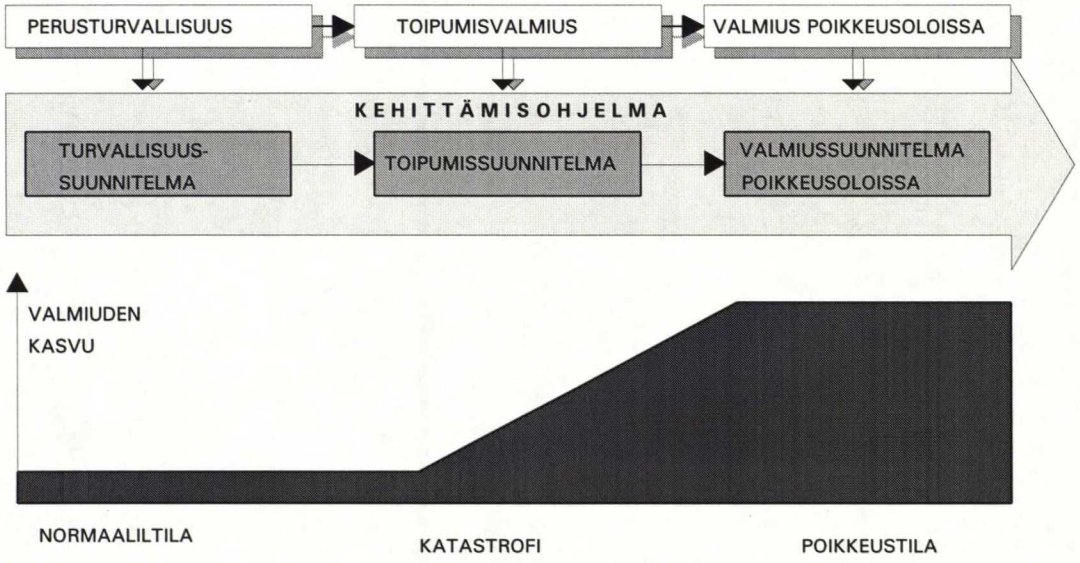
Käyttäjät ovat vastuussa omalta osaltaan tietoturvaohjeiden noudattamisesta, oman osaamisen ja tietämyksen tason ylläpidosta. Käyttäjien tulee myös raportoida havaitsemistaan riskeistä tai tietoturvaa uhkaavista tekijöistä osaston vastuuhenkilölle tai atk-osastolle.

4.2
Tietoturvan kehittämissuunnitelma

Tietoturvan kehittämissuunnitelmassa on määriteltävä elintärkeät tietojärjestelmät ja tietoturvapolitiikkaan pohjautuen luotava periaatteet ja vaatimukset perusturvallisuudelle, toipumiselle ja valmiudelle poikkeusoloissa. Samoin on otettava kantaa tietojärjestelmän fyysisen suojan, laitteistojen, ohjelmistojen, tiedon ja tiedonsiirron suojauksen kehittämiseen ja ylläpitämiseen.

Organisaation tietojärjestelmän turvaamisen tarpeet voidaan jakaa yrityksen normaalien toimintaolosuhteiden vaatimiin turvallisuustoimenpiteisiin ja toiminnan varmistamiseen poikkeusoloissa. Poikkeusolot voivat muodostua joko äkillisistä, yksittäisistä katastrofeista (tulipalo, vesivahingot tms.) tai pitempiaikaisemmista poikkeustilanteista (sota, lakko tms.). Äkillisissä, lyhyempiaikaisissa katastrofeissa on tärkeintä vahinkojen rajoittaminen ja toimintakyvyn palauttaminen ennalleen, kun taas pitempiaikaisissa poikkeustilanteissa on tärkeää toimintojen sopeuttaminen ja toiminnan jatkaminen poikkeusoloissa.

Kuvio 10 Tietoturvan kehittämisohjelma

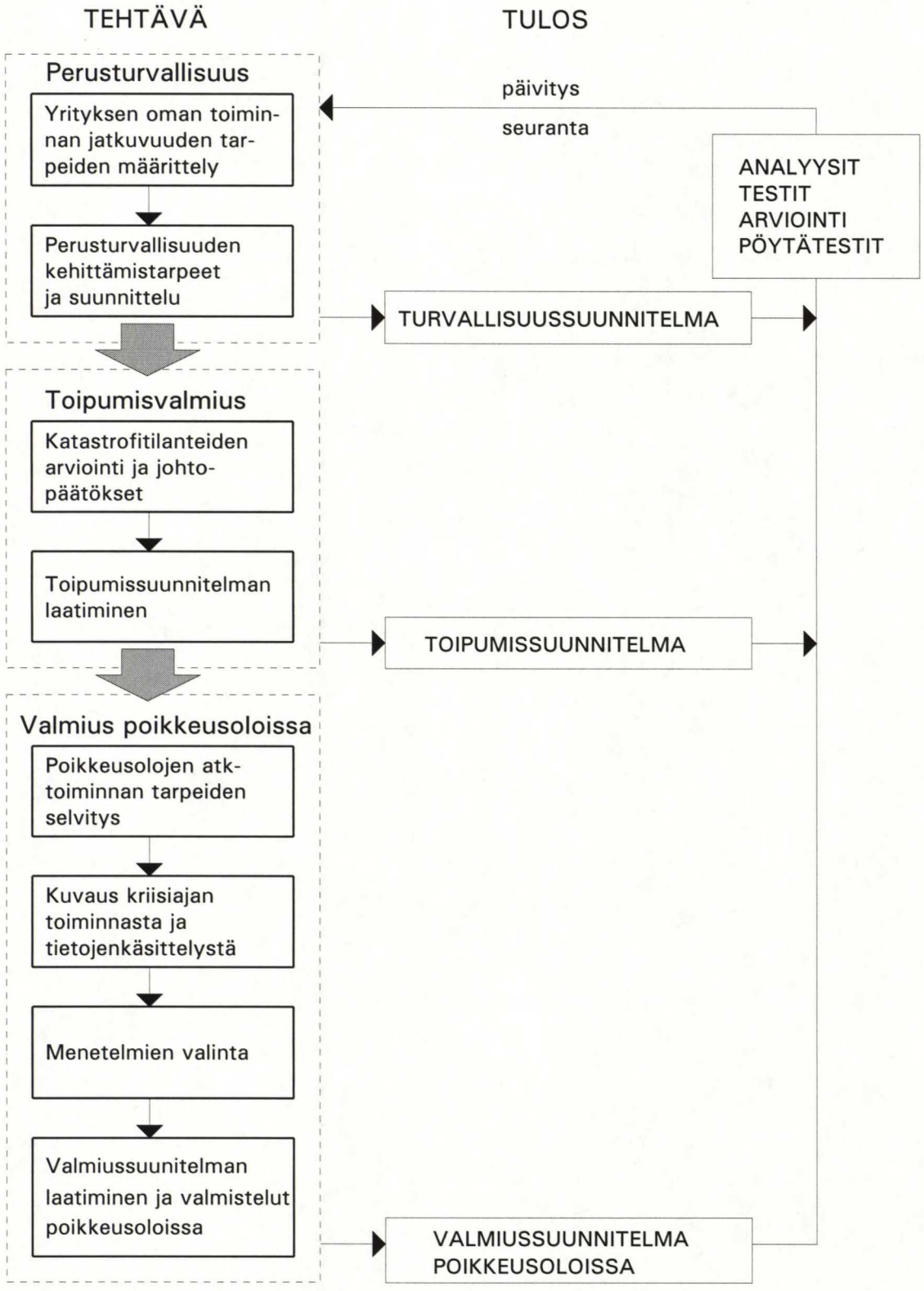


Lähde: Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu s. 5

Kehittämissuunnitelma voidaankin jakaa edellä mainituin perustein turvallisuussuunnitelmaan (normaaliolojen perusturvallisuus), toipumissuunnitelmaan (äkilliset, yksittäiset katastrofit; toipumisvalmius) ja valmiussuunnitelmaan poikkeusolojen varalle. Tarkka rajanveto eri suunnitelmien välillä voi olla vaikeaa, koska ne ovat riippuvaisia toisistaan ja tukevat toisiaan sekä järjestelmän riskitekijät ovat molemmissa tapauksissa samantyyppisiä.

Valmiuden kehittäminen on jatkuva prosessi, jossa tulee huomioida järjestelmän, ympäröivien riskien ja uhkien muutoksien lisäksi myös organisaation muun toiminnan ja tavoitteiden muuttuminen. Muutoksien tulisi heijastua tietoturvapolitiikan kautta tietoturvan toteuttamiseen ja tavoitteisiin.

Kuvio 11 Valmiussuunnittelu



Lähde: Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu s. 7

4.2.1

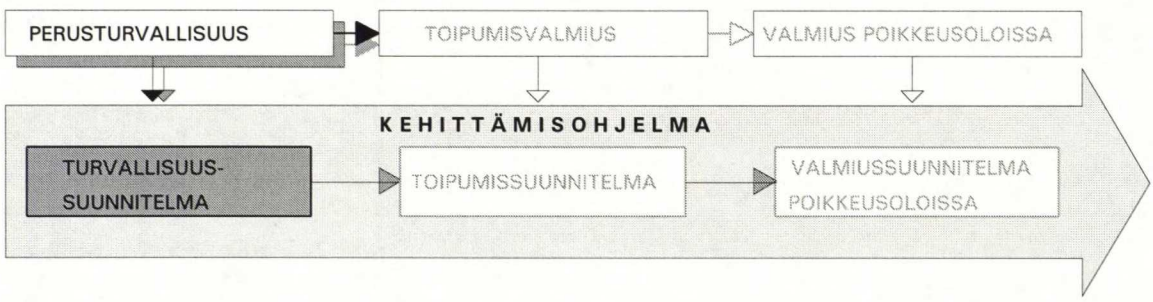
Turvallisuussuunnitelma

Turvallisuussuunnitelman tehtävänä on taata tietojärjestelmän perusturvallisuus sillä tasolla, kuin se yrityksen ja tietojärjestelmän toiminnan kannalta on määritelty. Tietojärjestelmien tehokas suojaus on toteutettavissa vain mikäli yrityksen tietoturvapolitiikka on määritelty ja johto on sitoutunut sen toteuttamiseen. Toimenpiteiden tulee perustua yksityiskohtaiseen turvallisuussuunnitelmaan ja henkilökunta on perehdytettävä ohjeiden noudattamiseen. Turvallisuutta on myös kehitettävä osana muuta järjestelmäkehitystä ja on huomioitava, että perusturvallisuuden on taattava järjestelmän käytön jatkuvuus normaalioloissa. Perusturvallisuuden luominen on turvallisuuden kehittämisen päätavoitteita ja kuulu olennaisena osana hyvään tietojenkäsittelytapaan.

Perusturvallisuus on otettava huomioon laite- ja ohjelmistopolitiikassa sekä atk-avainhenkilöpolitiikassa. Samoin perusturvallisuus kattaa tietojärjestelmän fyysisen suojauksen laitteistojen, ohjelmistojen ja käyttöjärjestelmän kannalta sekä järjestelmässä käsiteltävän tiedon ja tiedonsiirron suojauksen.

Tämän mukaan tulisi varmistaa, että järjestelmässä käsiteltävät tiedot on luokiteltu luottamuksellisuuden ja käytön vaatimusten mukaan ja että tiedostoihin ja palveluihin pääsevät vain hyväksytyt valtuudet omaavat henkilöt.

Kuvio 12 Perusturvallisuus



Tietojärjestelmään sekä tietojenkäsittelytiloihin pääsy ulkopuolisilta on oltava estetty ja valvottu ja laitteiston on oltava fyysisesti suojattu luvattoman tunkeutumisen tai onnettomuuksien varalta.

Organisaation sisäinen ja ulkoinen tiedonsiirto pitää olla suojattu fyysisten vahinkojen, tunkeutumisten, paljastumisen ja tiedon muuntumisen varalta.

Ohjelmien ja tietojen jatkuva käytettävyys tulisi varmistaa varmuuskopioinnilla sekä varajärjestelmillä. Myös atk-avainhenkilöiden työhönotolle ja sijaisuuksien järjestämiseen sekä henkilöstön motivoinnille on luotava menetelmät, jotka takaavat tietojärjestelmän käytön ja kehittämisen jatkuvuuden.

Atk-hankintojen yhteydessä on varmistettava varalaitteiden ja -tarvikkeiden saatavuus sekä korvaavien laitteiden ja ohjelmistojen yhteensopivuus olemassaolevien laitteiden ja järjestelmien kanssa. Laite- ja ohjelmistotoimittajien valinta on varsinkin järjestelmälle kriittisten toimintojen ja laitteiden kannalta tehtävä huolella. Toimittajien valinnassa on huomioitava luotettavuus, asiantuntemus ja toiminnan jatkuvuus, jolloin taataan nopea huollon ja varaosien saaminen sekä huollon käytettävyys kriisitilanteissa. Erilaisilla hankinta-, toimitus- tai huoltosopimuksilla saattaa olla perusturvallisuutta tukeva vaikutus.

Atk-henkilökunta vastaa tietojenkäsittelyn kriittisimmistä tehtävistä. Tietojenkäsittelyn henkilöstöresurssien varmistaminen edellyttää ainakin seuraavia toimenpiteitä:

- palkattavan atk-henkilöstön luotettavuuden ja ammattitaidon varmistaminen
- selkeää tehtäväkuvausta myös turvallisuusvastuista
- kirjallista työsopimusta ja vaitiololupausta
- jatkuvuuden varmistavia henkilöstöjärjestelyjä
- sijaisuuksien varmistamista
- ammattitaidon ylläpitoa (koulutus)

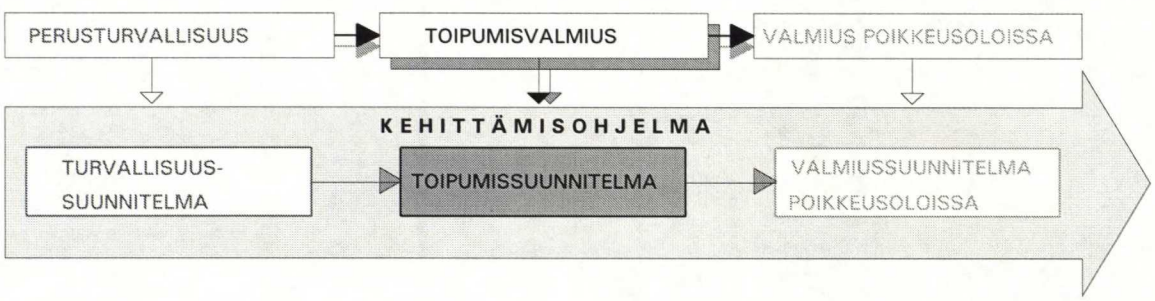
4.2.2

Toipumissuunnitelma

Toipumissuunnitelman tavoitteena on tietojenkäsittelyn vakavasta keskeytyksestä seuraavien vahinkojen vähentäminen; toipumisvalmiuden luominen ja ylläpitäminen. Tämä pyritään aikaansaamaan jatkamalla toiminnalle elintärkeitä tietojenkäsittelytoimintoja tilapäisjärjestelyin sekä takaamalla mahdollisimman nopea palautuminen toiminnan vaatimalle tuotantotasolle. Tällä tavalla suunnitelmalla luodaan ennalta perusta toipumiselle.

Suunnitelman on sisällettävä riittävät kuvaukset ja määritykset, joilla luodaan perusta toipumisvalmiuden vaatimille toimenpiteille katastrofista toipumisen varalle. Toipumisvalmiudella luodaan perusta myös valmiussuunnittelulle poikkeusolojen varalle.

Kuvio 13 Toipumisvalmius



Toipumissuunnitelma määrittelee elintärkeille tietojärjestelmille suurimmat sallitut keskeytysajat, varajärjestelmävaatimukset, huollolle asetettavat vaatimukset sekä varajärjestelmiin siirtymisajat. Toipumissuunnitelman ja siihen liittyvien varalaite- ja varatilasopimusten tulee olla kirjallisia. Samoin suunnitelma määrittelee vastuun katastrofitilanteen arvioinnista ja tarvittavien toimenpiteiden toteuttamisesta. Suunnitelma on myös testattava.

Toipumisaikaan liittyvät vaatimukset, vastuut ja toimenpiteet valmiuden luomiseksi on selvitettävä ennalta suunnitelmaa varten sekä on tehtävä vaadittavat testaukset suunnitelman toimivuuden takaamiseksi.

Suunnitelman on katettava sekä varsinainen suunnitelman toimeenpano että palaaminen normaalitoimintaan sekä ohjeet toiminnasta erilaisissa keskeytystilanteissa. Myös seuranta ja raportointi on hoidettava suunnitelman toteutumisen aikana.

Toipumissuunnitelma sisältää:

- toiminnan kannalta elintärkeiden tietojärjestelmien ja sovellusten määrittelyn
- kuvauksen tapahtumista, jotka saattavat johtaa toiminnan katastrofinomaiseen keskeytykseen
- elintärkeät toiminnot ja niille määritellyt suurimmat sallitut keskeytysajat korvaaviin järjestelmiin siirtymiseksi
- valmiusorganisaatio
- vastuut toipumissuunnitelman käynnistämisestä ja toimenpiteistä
- vastuuhenkilöiden hälyttämisen
- yhteyshenkilöt
- ohjeet laitteiden ja ohjelmien pelastamisesta

4.2.3
Valmiussuunnitelma

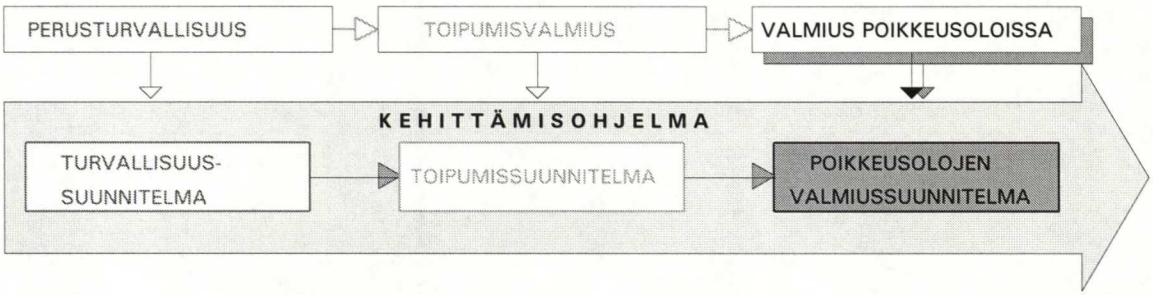
Tietojenkäsittelyn valmiuden tavoitteena poikkeusoloissa on organisaatiolle välttämättömien tietojenkäsittelytoimintojen ylläpitäminen mahdollisimman hyvin vakavissakin kriisitilanteissa. Toimintakyvyn säilyttäminen ei ole mahdollista ilman riittävän pitkälle tehtyjä valmisteluja ja varauksia.

Toipumisvalmius käsittää:

- toiminnan jatkamisen varajärjestelmin keskeytyksen jälkeen
- palautumisen normaalitoimintaan.
- varajärjestelmien testauksen
- reunaehdot ja ohjeet suunnitelman käynnistämisestä ja toimeenpanosta

- henkilökunnan koulutuksen toipumissuunnitelman edellyttämiin toimenpiteisiin

Kuvio 14 Valmius poikkeusoloissa

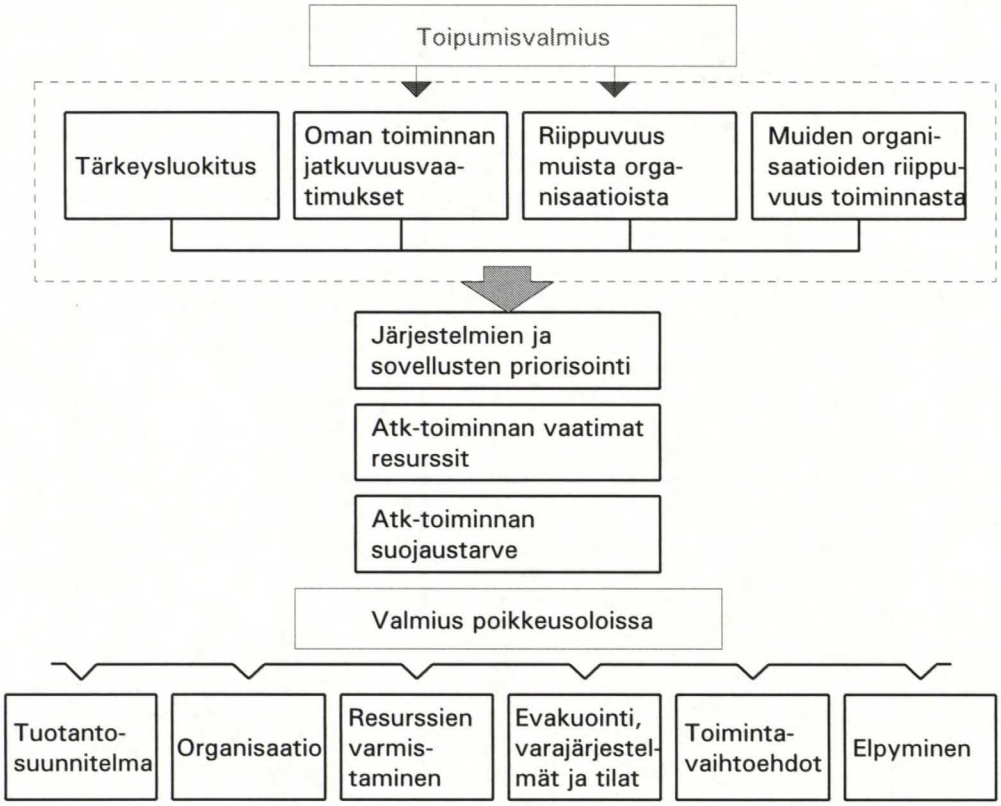


Poikkeusolojen aikainen tietojenkäsittelyn perustaksi tulee virastojen, laitosten sekä elinkeinoelämän yritysten ja järjestöjen määritellä toimintansa poikkeusoloissa pohjautuen perushuoltojärjestelmien ylläpitovaatimuksiin. Yritysten tärkeysluokittelu on eräs tavoiteasettelun lähtökohta. Tavoitteisiin sisältyy myös toiminnan elvyttäminen kriisin väistyttyä.

Pitkäaikaisen kriisin varalta on suunniteltava myös manuaalitoiminnat siltä varalta, että atk:ta ei pystytä ylläpitämään. Tämä vaihtoehto on aina otettava huomioon, vaikka ensisijaisesti pyritään ainakin tärkeimmät toiminnot hoitamaan atk:lla kaikissa tilanteissa.

Valmiussuunnitelma kohottaa perusturvallisuuden ja toipumissuunnitelman toimenpiteet vaikeiden kriisitilanteiden vaatimalle tasolle. Perusteet valmiuden suunnittelulle poikkeusoloissa antaa johdon saama kokonaiskuva poikkeusolojen vaikutuksista ja sen pohjalta tehty arvio valmiussuunnittelun tarpeesta ja alustavista tavoitteista. Suunnitelmaa tehtäessä on otettava huomioon myös yritysten tärkeysluokituksesta ja valmiussuunnittelusta vastaavien viranomaisten vaatimukset ja odotukset. Johdon tehtäviin kuuluu myös valmiussuunnittelun käynnistäminen johdon nimeämän vastuuhenkilön johdolla.

Kuvio 15 Toipumisvalmius poikkeusoloissa

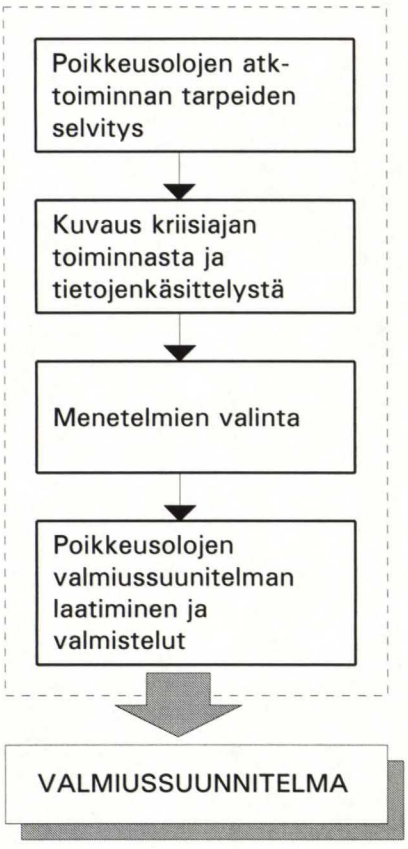


Valmiussuunnitelmassa tulisi selvittää ainakin olemassa olevat edellytykset toimia eri asteisissa poikkeusoloissa. Tähän vaikuttaa organisaation sisällä henkilöresurssien varmuus ja atk:n käyttövarmuus. Organisaation ulkopuolisina vaikuttajina ovat tiedonsiirron keskeytysten vaikutus toimintaan sekä huollon, varaosien ja tarvikkeiden saanti ja riittävyys eri tilanteissa.

Valmiustavoitteiden määrittely:

- mikä on organisaation ja sen toiminnan merkitys kansalaisten toimeentulolle ja elinkeinoelämälle
- mihin tärkeysluokkaan yritys kuuluu, yhteiskunnan odotukset tai vaatimukset toiminnalle kriisitilanteessa
- miten yritys haluaa toimia kriisitilanteessa
- avainalueiden valmiustavoitteet
- tukitoimintojen valmiustavoitteet
- tarvittavat resurssit
- tietojärjestelmien valmiustavoitteet

Kuvio 16 Valmiussuunnittelu poikkeusoloissa



Poikkeusolojen häiriöt ja uhat kohdistuvat pahimmin henkilöstöön, laitteistoihin, tietoliikenteeseen ja huoltoon. Resurssien supistumiseen vaikuttavat esim. erilaisia poikkeusoloja varten säädetyt lait ja asetukset (väestönsuojelulaki, säännöstelyvaltuuslaki, liikekannallepano, sotalaki yms.), jolloin osa henkilökunnasta tai yrityksen koneista ja laitteista voidaan joutua luovuttamaan valtioneuvoston tai sotilasviranomaisten käyttöön.

Kokonaisuudessaan poikkeusolojen vaikutukset organisaation ja tietojärjestelmän toimintaan ovat selvästi laajempia ja monitahoisempia kuin yksittäisten onnettomuuksien vaikutukset. Tästä syystä selviytyminen poikkeusolojen vaatimuksista edellyttää suurempaa joustavuutta ja valmiutta toiminnan mukauttamiseen.

Kun organisaation tavoitteet ja toimintaympäristö poikkeusoloissa on määritetty, voidaan tietojärjestelmät ja atk-sovellukset jakaa eri ryhmiin niiden

kriittisyyden perusteella. Ensimmäiseen tärkeysryhmään kuuluvat sellaiset järjestelmät ja sovellukset, joiden tukemat toiminnot ovat organisaatiolle välttämättömiä ja joille atk:n toimivuus on välttämättömyys. Toiseen ryhmään kuuluvat sellaiset sovellukset, joiden tukemaa toimintaa voidaan supistaa ja joissa atk on tarpeellinen, mutta myös atk:n käyttöä voidaan supistaa. Kolmanteen ryhmään kuuluvat sellaiset sovellusalueet, jotka voidaan korvata esim. manuaalitoiminnoilla tai lopettaa kokonaan. Prioriteetin mukaan eri sovellusryhmille määritetään tämän jälkeen palvelutasovaatimukset (valmiusvaatimukset; järjestelmän käytettävyys, katkokset, manuaalitoiminnot jne).

Atk-henkilö- ja laiteresurssien jako eri systeemien ja sovellusten kesken vaikuttaa myös haluttuun järjestelmän palvelutasoon. Resurssien jakamista suunniteltaessa on muistettava ottaa huomioon myös varalaite- ja varahenkilötarpeet. Atk-toiminnan suojaustarve on määritettävä kokonaisuudessaan ja varmistettava ainakin päätoimintojen jatkamisen edellytykset (henkilöstö ja sen ammattitaito, tarvikkeet, toimitilat ja tarvittavat palvelut). Varajärjestelmiä suunniteltaessa on muistettava, että manuaalijärjestelmät tarvitsevat lähes poikkeuksetta enemmän työvoimaa toimiakseen kuin vastaavat atk-järjestelmät. Toimintaa sopeutettaessa voidaan atk:n käyttöastetta alentaa portaittain. Tällöin seurataan valmiussuunnitelmassa määriteltyjä toimintojen ja sovellusten tärkeysluokittelua. Suunnitelmassa on otettava huomioon myös mahdollinen evakuointi ja toiminnan siirtäminen muualle tilapäisesti tai pysyvästi sekä arvioitava myös koko toiminnan keskeyttämisen vaikutukset.

Valmiussuunnitelma sisältää myös elpymisen poikkeusoloista. Toimintaa ja atk:ta purettaessa kriisin aikana on otettava huomioon myös toiminnan elvyttäminen kriisin lauettua. Laitteistot, tiedot ja tarvikkeet on varastoitava siten, että ne säilyvät käyttökelpoisina, jotta normaalitoimintoihin palaaminen sujuu vaikeuksitta.

5
TAKUUKESKUKSEN LIIKETOIMINTA- JA TIETOHALLINTOSTRATEGIAN VAIKUTUS TIETOTURVAAN

Organisaation tietoturvan tason määrittäminen ja sen toteuttaminen perustuu organisaation liiketoimintaan ja sen tietojärjestelmiin. Tietoturvallisuutta ei voida tehokkaasti kehittää tai ylläpitää irrallisena toimintona vaan sen on pohjauduttava organisaation liiketoimintaan ja sen tavoitteisiin ja strategioihin. Esimerkiksi liiketoiminnan alue ja tietojärjestelmien laajuus antavat suoraan viitteitä tietoturvalle asetettavista vaatimuksista; voidaan olettaa, että pankkitoimintaa harjoittava ja suuren atk-järjestelmän omistava yritys asettaa tietojärjestelmien tietoturvallisuudelle suuremman painon kuin koneen osia valmistava metallialan yritys. Tietojärjestelmän koosta tai tärkeydestä riippumatta tulisi kuitenkin järjestelmän suojaamisesta tehdä tietoinen päätös, jonka pohjalta voidaan häiriötilanteissa toimia. Vaikka "tietojärjestelmä" käsittäisi vain yhden mikron, on varmasti kannattavaa suojata laite ja varmistaa sen sisältämät tiedot sekä ohjelmat.

5.1
Takuukeskuksen toiminnan kuvaus

Valtiontakuukeskus perustettiin 1.9.1989 yhdistämällä Vientitakuulaitos (VTL) ja Valtiontakauslaitos (VATA). Vanhojen laitosten henkilökunta, vastuu ja velvollisuudet siirtyivät sellaisinaan Takuukeskukselle. Valtiontakuukeskuksen tehtävänä on harjoittaa rahoitustoimintaa myöntämällä takuita ja takauksia sekä parantaa ensisijassa pienten ja keskisuurten yritysten riskirahoituksen saatavuutta, edistää kannattavaa vientiä ja parantaa kotimaisen teollisuuden sekä eräiden muiden elinkeinoalojen yritystoiminnan kilpailukykyä ja kehittämisedellytyksiä noudattaen Takuukeskuksen toimintaa sääteleviä lakeja ja asetuksia. Tämä tapahtuu tarjoamalla viejille ja viennin rahoittajille suojaa kansainvälisen toiminnan tuomia riskejä vastaan sekä tukemalla pienten ja keskisuurten yritysten riskirahoituksen saatavuutta, edistämällä laivanrakennus- ja laivanvarustamotoimintaa, teollisuuden

ympäristönsuojeluinvestointeja sekä turvaamalla kotimaista perusraaka-ainehuoltoa. Takuukeskuksen palveluksessa on n. 150 toimihenkilöä. Helsingin lisäksi Takuukeskus toimii Lahdessa, Oulussa, Tampereella, Turussa ja Seinäjoella sijaitsevien alueyksiköiden kautta.

Toimintoprosessit

Takuukeskuksen toiminta voidaan jakaa kuuteen eri prosessiin:

1 Kotimaiset takaukset

2 Vientitakuut

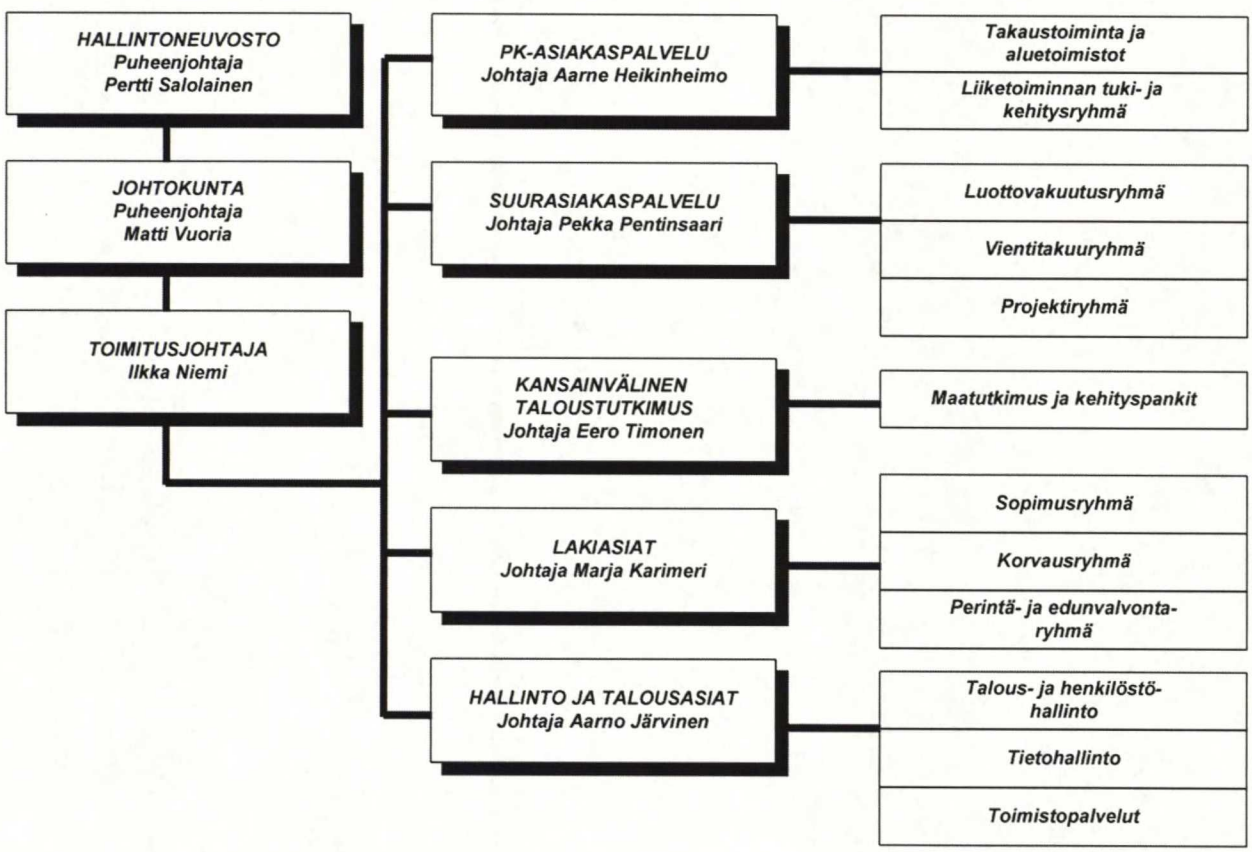
3 Kansainvälinen taloustutkimus ja maariskit

4 Sopimusjuridiikka

5 Korvaus ja takaisinperintä

6 Hallinto-, talous- ja henkilöstöasiat

Kuvio 17 Takuukeskuksen organisaatiokaavio 12/1994



TAKUUKESKUKSEN SIDOSRYHMÄT

Ohessa on listaus Takuukeskuksen sidosryhmistä, joiden kanssa on säännöllistä ja toistuvaa tietojen vaihtoa.

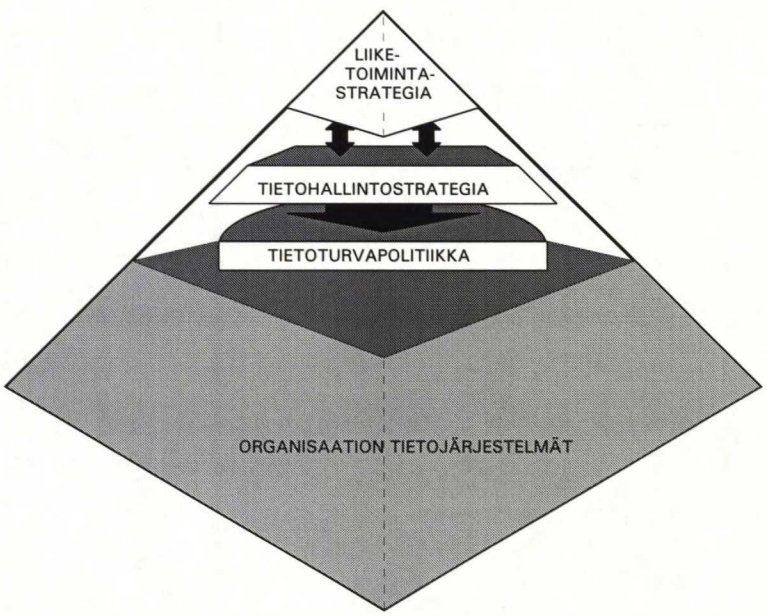
TAKUUKESKUS	VALTIONHALLINTO	KOTIMAISET YHTEYDET	KANSAINVÄLISET YHTEYDET
johto; hallintoneuvosto, johtokunta, toimitusjohtaja	Eduskunta ja valtioneuvosto	Asiakasyritykset: pörssiyhtiöt, pk-yritykset, varustamot ym.	Maailmanpankki
takuuosasto	Kauppa- ja teollisuusministeriö	Luotonantajat: pankit, vakuutusyhtiöt, Suomen Vientiluotto ym.	IMF
yritystutkimus	Ulkoministeriö	Muut riskirahoittajat: KERA Oy, TEKES, Sitra	OECD-jäsenmaat
maatutkimus	Valtionvarainministeriö	Luottotietoyhtiöt, Suomen luotonantajain Osuuskunta, Asiakastieto Oy ym.	Bernin Unionin
sopimusjuridiikka	Suomen Pankki	Perintätoimistot	Pohjoismaiden takuulaitokset
korvaukset ja perintä	Valtionkonttori		Luottotietoyhtiöt ja -pankit, Esselte Global Scan ym.
talous	Postipankki		
tietohallinto	Ulkomaankauppaliitto		
	Vientikoulutussäätiö		
	Vtkk		
	Tilastokeskus		
	Patentti- ja rekisterihallitus		

5.2

Liiketoimintastrategian vaikutus tietohallintostrategiaan

Organisaatio, joka toimintansa tukena käyttää automaattista tietojenkäsittelyä, on tehnyt strategisen päätöksen tietojenkäsittelyn hyödyntämisestä omassa toiminnassaan. Yleensä tavoitteeksi on asetettu toiminnan tehostaminen, kustannussäästöt ja palvelujen parantaminen. Tällaiset päätökset ja strategiset tavoitteet tulevat lähes poikkeuksetta organisaation johdolta, jolloin on selvää että tietojenkäsittelyn ja tietojärjestelmien kehittämisen strategiat noudattavat organisaation kokonaisstrategioita ja tukevat tavoitteiden saavuttamista. Tietoturva on osa tietojenkäsittelyä, mutta se ei ole pelkästään teknisten turvatoimenpiteiden toteuttamista vaan myös päätös tietystä toimintapolitiikasta liittyen sekä organisaation että tietojenkäsittelyn strategiaan.

Kuvio 18 Tietoturvapolitiikka liiketoimintastrategian osana



Takuukeskus on tietoyritys, jonka toiminta perustuu tietojenkäsittelyyn. Takuu- ja takaustoiminnan uudelleenorganisointi sekä muutokset toimintaympäristössä niin koti- kuin ulkomaillakin tuovat uusia vaatimuksia Takuukeskuksen liiketoiminnalle ja sitä kautta myös tietojärjestelmille ja niiden kehittämiselle. Rahoituspalvelut muuttuvat tietopalveluiksi, joita asiakkaat voivat hoitaa omilta päätteiltään, jolloin tietojenkäsittelyn automatisointi rahoitustoiminnassa

lisääntyy voimakkaasti. Takuukeskuksen toiminta kehittyy samaan suuntaan siten, että se tulee yhä selvemmin osaksi muita markkinoiden rahoituspalveluita, jolloin toimiva ja joustava tietojärjestelmä luo edellytykset toimia kilpailukykyisesti ja asiakkaita hyvin palvellen.

Takuukeskuksessa tehtiin 1990 - 1991 tietojenkäsittelyn kokonaistutkimus, jossa käytettiin Helsingin kauppakorkeakoulussa tietojenkäsittelyn strategisen suunnittelun tueksi kehitettyä METO 3 -viitekehystä. Kokonaistutkimuksen tavoitteina oli tietojenkäsittelyn kehittämisen yleisten tavoitteiden ja pitkän aikavälin tietohallintostrategian luominen siten, että ne tukevat mahdollisimman hyvin Takuukeskuksen muun toiminnan päämääriä sekä parantaa tietojärjestelmien joustavuutta ja häiriötöntä toimintaa riippumatta organisaation ja sen johtamisjärjestelmien muutoksista. Koska tietoturvapolitiikka pohjautuu tietohallintostrategiaan ja sen toteutusympäristö, organisaation tietojärjestelmä, määrittyy sekä tietojärjestelmän infrastruktuurin että strategisten puitteiden mukaisesti, on nämä otettava tietoturvapolitiikkaa luotaessa huomioon.

Keskeisenä tietohallinnon strategisena lähtökohtana on yhdistää liiketoiminta ja tietojenkäsittelyn kokonaisarkkitehtuuri tukemaan Takuukeskuksen toiminnan päämääriä. Tietohallinto keskittyy lähivuosina yhtenäistämään Takuukeskuksen tietojenkäsittelyn kokonaisarkkitehtuurin luomalla hajautetun tietojärjestelmän. Tuottavuuden kasvu pyritään saamaan aikaan kehittämällä toimistoautomaatiota voimakkaasti. Tuotantoprosessin automatisoinnilla parannetaan riskienhallintaa, palvelukykyä ja kustannustehokkuutta. Automatisoinnilla muutetaan työtapoja, mikä edellyttää henkilöstön uudelleenorientoitumista tehtäviinsä.

Tietohallinnon näkökulmasta tämä vaatii tietohallinnon suunnittelun ja ohjauksen tehostamista liiketoiminnan vastuuhenkilöiden ja tietohallinnon toteuttajien yhteistyötä kehittämällä. Tietohallintoresursseja on pystyttävä kohdistamaan tehokkaasti ja projektien priorisointi on suunniteltava liiketoiminnan kannalta parhaalla mahdollisella tavalla.

Yleisesti voidaan todeta, että tietohallinnon kehittäminen liiketoimintaa tukevana toimintona edellyttää aikaisempaa huomattavasti tiiviimpää liiketoimintastrategioiden ja tietohallinnon yhteensovittamista. Tietohallinto kytkee toisiinsa tietojenkäsittelyn eri osa-alueet; laitteet, sovellukset ja tietoliikenteen, yrityksen toimintaa mahdollisimman hyvin palvelevaksi kokonaisuudeksi. Tehokkaasti toteutettu tietohallinto ja tiedonhallintajärjestelmät, jotka mahdollistavat reaaliaikaisen ja oikean tiedon välittömän saatavuuden jokaiselle tiedon tarvitsijalle, on Takuukeskuksen kaltaisen informaatiota muokkaavan asiantuntijaorganisaation elinehto kiristyvässä kilpailutilanteessa.

Valittu ratkaisu vaati myös selkeää kannanottoa tietoturvallisuudesta ja sille asetettavista tavoitteista. Automaattisen tietojenkäsittelyn kasvaessa on tietojärjestelmän toiminta myös turvattava. Halutun tietoturvatason ja sen painopistealueiden määrittäminen kuuluu olennaisesti tietohallintostrategiaan, ja siihen on otettava kantaa myös koko yrityksen toimintastrategioita laadittaessa. Tietoturvan päämäärien ja tavoitteiden asettaminen ei voi tapahtua operatiivisella tasolla, vaan se on yrityksen johdon ja tietohallinnon johdon tehtävä.

Tietoturvallisuuden perusvaatimukseksi voidaan Valtiontakuukeskuksessa asettaa hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuuden luominen. Hyvään tietojenkäsittelytapaan kuuluu erottamattomasti tietoturvallisuus. Asianmukaista perusturvallisuuden tasoa tarvitaan, koska järjestelmän tiedot ja palvelut muodostavat taloudellisesti arvokkaan ja organisaation toiminnan kannalta tärkeän kokonaisuuden.

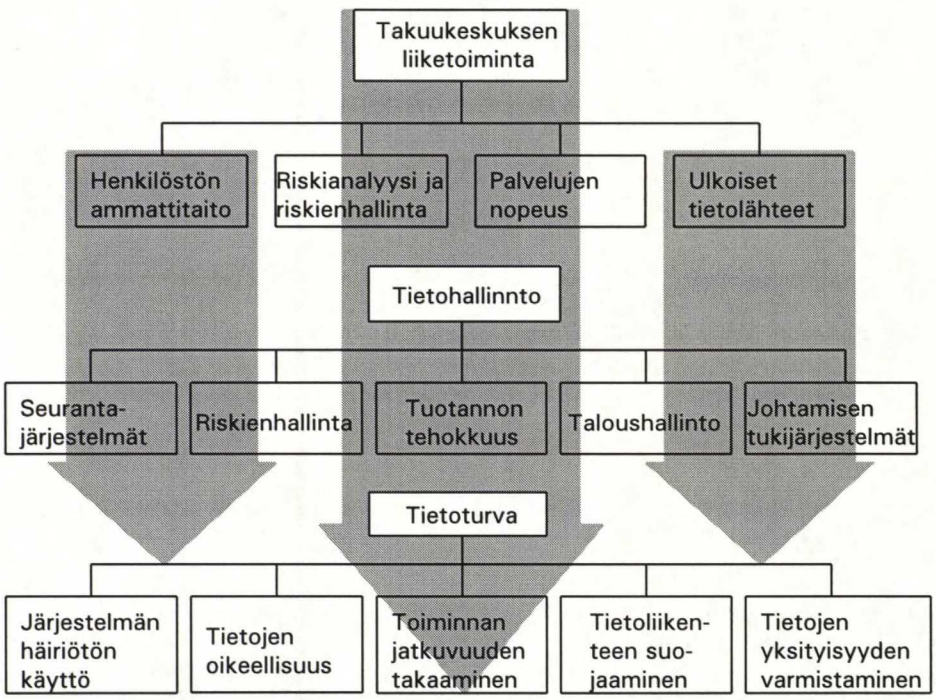
5.3
Tietohallinnon ja tietojenkäsittelyn strategia

Valtiontakuukeskuksen muodostaminen synnytti hyvin epäyhtenäisen atk-kulttuurin. Sekalaiset tietojärjestelmät pakottivat tekemään merkittäviä linjaratkaisuja. Samalla tarjoutui mahdollisuus kokonaan uuden tietohallintostrategian esittämiseen. Tuloksena syntyi täysin hajautettu

kokonaisarkkitehtuuri, jossa työskentely perustuu tehokkaisiin henkilökohtaisiin työasemiin ja paikallisverkkoon.

Työasemissa on graafinen käyttöliittymä, joka mahdollistaa sovellusten moniajon. Nopean paikallisverkon avulla on käytettävissä ulkoiset ja sisäiset tietokannat; datatiedostot, tekstiarkistot, kuvatiedostot sekä asiantuntijajärjestelmien sääntötietokannat. Kirjoitinpalvelijoiden avulla saa tekstiä, taulukoita, kirjapainotuotteita, kuvia, kalvoja ym. , myös värikuvina. Sisäinen tiedonsiirto hoidetaan omalta työasemalta paikallisverkon avulla ja ulkoiset yhteydet verkon tietoliikennepalvelimien avulla yleisiin paketti- ym. palveluverkkoihin. Ratkaisu mahdollistaa takuutoiminnan käsittelyprosessien lähes täydellisen automatisoinnin. Automatisointi edellyttää lisäksi nykyisten käsittelymenetelmien, tuotteiden sekä toimistoautomaation merkittävää edelleenkehittämistä.

Kuvio 19 Liiketoiminnan, tietohallinnon ja tietoturvan painopistealueet



Takuukeskuksen liiketoimintastrategian ja palveluideoiden mukaan tärkeimmät toimintojen painopistealueet ovat:

1. Henkilöstön ammattitaidon kehittäminen
2. Riskianalyysi ja riskienhallinta

3. Ulkoisten tietolähteiden käyttö
4. Palvelujen nopeuttaminen

Toimintojen osa-alueet, joissa tietohallinnolla on keskeinen merkitys:

1. Sisäiset seurantajärjestelmät
2. Riskienhallinta
3. Tuotannon tehokkuus
4. Taloushallinto
5. Johtamisen tukijärjestelmät

Liiketoimintayksiköissä tietojenkäsittelyn prioriteetit ovat tiedon siirron tehostamisessa organisaation sisällä ja sitä kautta myös päätöksenteon tukijärjestelmien kehittäminen; tiedon hankinta, tiedon analysointi, tiedon muokkaus.

Tietojenkäsittelyn prioriteeteistä on johdettu tietoturvan osa-alueet, jotka on erityisesti huomioitava. Näitä osa-alueita ovat järjestelmän häiriötön käyttö, tietojen oikeellisuuden varmistaminen ja toiminnan jatkuvuuden takaaminen. Myös tietojen yksityisyyden varmistaminen sekä tietoliikenteen suojaaminen kuuluvat tietoturvassa painottuviin asioihin.

Tietohallinnon kannalta tärkeät / korostuvat asiat:
-tietojärjestelmien yhtenäistäminen; tietovarastot, sovellukset, tekniset järjestelmät sekä tietoliikenne ratkaisut on perustuttava yhteiseen, standardinomaiseen ratkaisuun, jolla taataan järjestelmän häiriötön toiminta.
-nopeat tulokset; riippuu tahdosta sekä henkisistä ja taloudellisista resursseista.
-joustavuus; varauduttava liiketoiminnan ja/tai toiminta ympäristön muutoksiin, hajautetuilla ja varmennetuilla tietojärjestelmillä ja tehokkaalla viestinnällä.
-henkilöstön koulutus; omaksuttava uudet metodit ja apuvälineet, sekä oma vastuu tietojärjestelmän toimivuudesta. Koulutus portaittain ja selektiivisesti.
-kehittäminen; kyettävä vastaamaan nykyisiin ja uusiin haasteisiin laadittujen strategioiden pohjalta

-ylläpito; huolehdittava jokapäiväisistä ongelmista ja vastattava järjestelmän toimivuudesta sekä pyrittävä luomaan luotettava järjestelmä pyrkimällä ennakoimaan riskit ja uhat
-dokumentointi; hyvällä dokumentoinnilla vähennetään ylläpito- ja koulutustarvetta sekä kriisi- tai ongelmatilanteissa luodaan edellytykset nopealle toipumiselle ja normaalitoiminnan palauttamiselle

Mahdollisuudet ja rajoitukset asetettujen tavoitteiden saavuttamiseksi tulevat lähinnä resurssien riittävyyden ja laadun taholta: henkiset resurssit sekä tekniset ja taloudelliset resurssit. Samoin organisaation asenteet ja tottumukset vaikuttavat organisaation sitoutumiseen ja tavoitteiden saavuttamiseen.

5.3.1 Tietohallinnon toiminta-ajatus

Tietohallinnon toiminta-ajatuksena on kehittää ja ylläpitää automaattisen tietojenkäsittelyn menetelmiä ja apuvälineitä siten, että voitaisiin entistä paremmin hyödyntää Takuukeskuksen käytettävissä olevia tietovarantoja linjojen liiketoimintastrategioita toteutettaessa.

Tietojenkäsittelyn kehittämisen keskeiset päämäärät ovat pysyvän kilpailuedun aikaansaaminen, riskienhallinnan kehittäminen sekä tuottavuuden parantaminen. Pysyvän kilpailuedun aikaansaamiseksi tarvitaan tietojärjestelmä, joka mahdollistaa tehokkaamman ja nopeamman asiakaspalvelun, esim. suoraan asiakkaan päätteeltä. Luotettavuuden ja laadun paraneminen säästää kustannuksia sekä parantaa Takuukeskuksen imagoa sekä riskienhallinnan kehittämisellä pyritään luottotappioiden pienentämiseen.

Palvelujen saatavuuden ja luotettavuuden turvaamisessa on tietoturvallisuudella keskeinen asema. Järjestelmän toiminta, tietojen oikeellisuus ja saatavuus on varmistettava ja varauduttava ennalta mahdollisiin käytön häiriöihin. Mikäli turvallisuuskysymyksiä ei huomioida riittävän hyvin pienetkin järjestelmän häiriöt näkyvät asiakkaille ja Takuukeskuksen ja sen

toimintojen luotettavuus kärsii. Asiakaskontaktit ovat luottamuksellisia eivätkä käsiteltävät tiedot saa joutua väärin käsiin. Riskienhallinnan ja päätöksenteon kannalta tietojärjestelmän tuottamien tietojen luotettavuus ja eheys ovat elintärkeitä.

5.3.2
Atk-hankinnat -ostopolitiikka

Atk-hankinnoissa keskitytään muutamiin tunnettuihin tuotemerkkeihin ja yhtenäinen laitestandardi teknisten ratkaisujen osalta on määräävä valintatekijä. Pääasiallisia laite- ja ohjelmistotoimittajia tulee olemaan kaksi tai kolme. Hankintoja tehtäessä otetaan huomioon toisaalta määräalennukset, toisaalta hankitun laitteiston tai ohjelmiston välitön käyttöönotettavuus. Laitteiden vaihdossa toteutetaan kierrätystä siten, että vanhat laitteet siirretään aina vähemmän tärkeisiin käyttökohteisiin.

Tietoturvan kannalta laitehankintoihin vaikuttaa mm. huollon, varaosien, teknisen tuen ja varalaitteiden saanti sekä laitetoimittajan maine ja taloudellinen tilanne. Toimittajien luotettavuus ja laitestandardit tukevat järjestelmän ylläpitoa ja toimintakyvyn säilyttämistä myös kriisitilanteissa. Vaikka tilausten ja ostojen keskittämisellä yhdelle toimittajalle saavutettaisiin kustannusetuja, aiheuttaa se kuitenkin riippuvuutta valitusta toimittajasta. Toiminnan jatkuvuuden takaamiseksi on turvallisempaa pitää yhteyksiä useampaan toimittajaan. Laitestandardien noudattaminen parantaa laitteiden yhteensopivuutta ja huoltoa. Samoin riippuvuus tietystä tuotemerkistä vähenee, jos saatavilla on muita vaaditut standardit täyttäviä laitteita.

Sovelluksia valittaessa keskeinen kriteeri on sellaisten valmisohjelmistojen käyttö, jotka tukevat hyvin liiketoimintaa, mutta joiden sovelluskohtainen räätälöinti on minimaalista. Muita tekijöitä ovat sovellusten yhteensopivuus käyttöliittymien kanssa ja sovellusten keskinäiset tiedonsiirto-ominaisuudet.

Sovellusten vaatima ylläpito ja niiden keskinäinen yhteensopivuus vaikuttaa koko järjestelmän toimintaan. Sovelluksia hankittaessa on tärkeää muistaa,

että niillä tuotetaan ja käsitellään kaikki yrityksen tarvitsema tieto. Tietojen eheyden ja luotettavuuden säilyttämisessä on oikeiden sovellusten valinta oikeisiin tehtäviin tärkeällä sijalla. Yleisesti tunnetut ja markkinoilla pitempään olleet tuotteet ovat yleensä toiminnoiltaan luotettavampia kuin uudet, juuri kehitetyt tuotteet, joista ei ole käyttökokemuksia. Ennen sovellusten hankintaa niiden toiminta ja sopivuus tulee testata yrityksessä. Sovellusten valintaan vaikuttaa myös käyttöohjeiden laatu, ohjelmiston käytön helppous ja selkeys, ohjelmalliset tarkistukset sekä päivitettävyys. Käyttäjän kannalta selkeä, hyvin ohjeistettu ja varmistuksilla varustettu ohjelma vähentää käyttövirheitä. Ohjelman versionhallinnassa on huomioitava se, onko vanhempien versioiden tiedot ja tietokannat käytettävissä uudessa päivitetyssä versiossa.

5.3.3
Tiedonhallinnan organisointi

Tietovarastojen hallinta palautuu osittain osastoille, joiden vastuuhenkilöt vastaavat tietokantojen ylläpidosta. Hajautetut tietokannat ovat yhteiskäyttöisiä, ja raportointi tapahtuu tehokkailla raporttivälineillä suoraan käyttäjän päätteelle tai jopa konekielisenä tiedonsiirtona suoraan toiseen sovellukseen.

Tiedonhallinnan organisoinnissa tulee kiinnittää huomio seuraaviin tekijöihin:

- käytön vastuualueet; jokaisella tietopankilla tulee olla oma vastuuhenkilö
- hajautus/keskitys; tietopankit osastojen omassa/koko organisaation käytössä
- tärkeimmät omat tietovarastot sijoitetaan omille, tehokkaille, hyvin suojatuille ja varmistetuille tiedosto- ja tietokantapalvelimille
- tiedon oikeellisuus, varmistus ja suojaus hoidetaan yhtenäisten periaatteiden mukaisesti valvotusti
- käyttöoikeuksia myönnetään tarpeen mukaan

Takuukeskuksen liiketoiminta tulevina vuosina on pitkälle riippuvainen tehokkaasta tiedonsiirrosta. Kehittyneellä ja kattavalla ulkoisella ja sisäisellä tiedon siirrolla kevennetään ja nopeutetaan tuotannollisia prosesseja

olennaisesti. Tiedonsiirto tapahtuu kunkin työntekijän henkilökohtaisen työaseman kautta. Myös ulkoisten tietoliikennepalvelujen loppukäytön vastuu hajautetaan työntekijöille. Tietoliikenneratkaisu nähdään kokonaisvaltaisena, ts. se kattaa organisaation sisäisen tietoliikenteen eli lähiverkon kautta hoidettavat ulkoiset yhteydet sekä lisäksi sovellusten välisen tiedonsiirron.

Tietoliikenteen käytössä vastuu hankitun tiedon oikeellisuudesta on vaikeampi todeta, koska tiedon tuottajia voi olla useita ja tieto on saattanut kulkea monen eri tahon kautta. Omien työntekijöiden tulisi varmistua ainakin ensisijaisen tietolähteen oikeellisuudesta ja valita yhteistyökumppaneiksi tunnettuja ja luotettavia osapuolia sekä varmistaa sopimuksilla vastuukysymykset. Tietoliikenteen käytön valvonta, häiriö- ja ongelmatilanteiden seuranta on myös tietoliikenteen pääasiallisilla käyttäjillä, jolloin henkilövalinnat, asiantuntemus ja koulutus ovat merkittävässä asemassa.

6
VALTIONTAKUUKESKUKSEN TIETOJÄRJESTELMÄN KUVAUS

Valtiontakuukeskuksen kotimaan riskin linjan ja ulkomaan riskin linjan (ennen yhdistymistä VATA ja VTL) atk-hankinnat on tehty samoihin aikoihin. Huolimatta samasta laitevalmistajasta ratkaisujen perusfilosofia poikkesi olennaisesti toisistaan; kotimaan linjan tietojärjestelmä perustui mikroverkkoon sekä henkilökohtaisiin työasemiin, ulkomaan linjan tietojärjestelmä taas minikoneeseen ja pääteverkkoon. Takuu ja takaustoiminnan uudelleenorganisointi, muutokset toimintaympäristössä sekä Valtiontakuukeskuksen muodostaminen synnytti hyvin epäyhtenäisen atk-kulttuurin uudessa organisaatiossa. Sekalaiset tietojärjestelmät pakottivat tekemään merkittäviä linjaratkaisuja ja luomaan uuden tietohallintostrategian.

Tältä pohjalta muodostettu täysin hajautettu tietojärjestelmä perustuu tehokkaisiin henkilökohtaisiin työasemiin ja paikallisverkkoon. Järjestelmien yhdistäminen ja hajautetun järjestelmän luominen vaativat seurantajärjestelmien yhdistämistä ja uudistamista, toimistoautomaation

kehittämistä, teknisen infrastruktuurin modernisointia ja yhdistämistä sekä tietokantojen yhtenäistämistä ja tietokantastandardin luomisen. Työasemiin valittiin graafinen käyttöliittymä, joka mahdollistaa useiden sovellusten yhtäaikaisen käytön. Paikallisverkon avulla on käytettävissä ulkoiset ja sisäiset tietokannat ja verkkopalvelimien kautta järjestelmän palveluja voidaan tarjota kaikille tietojärjestelmän käyttäjille. Sisäinen tiedonsiirto hoidetaan omalta työasemalta paikallisverkon avulla ja ulkoiset yhteydet verkon tietoliikennepalvelimien avulla yleisiin palveluverkkoihin.

6.1 Valtiontakuukeskuksen tietojärjestelmän tekninen infrastruktuuri

Tällä hetkellä Valtiontakuukeskuksen tietojärjestelmien selkärangan muodostaa IBM-kaapeloinnilla toteutettu lähiverkko. Nykyisin verkko kattaa kaikki työpisteet (n. 150) ja siihen on liitetty kaikki työaseemat. Erilaisia palvelimia tai palvelinkoneita (tietoliikenne, tulostus, tiedosto, tietokanta, gateway, fax, telex, CD-ROM jne.) on verkkoon kytketty n. 30. Kaikki palvelut on tarvittaessa kaikkien käyttäjien saatavilla (käytännössä palveluja tarjotaan pääasiallisesti "vain tarpeeseen"-periaatteella sallimalla pääsy vain niihin ohjelmiin ja tietohin, joita käyttäjä työssään tarvitsee).

Fyysisesti verkko on jaettu kolmeen osaan kolmen eri kiinteistön välille. Kiinteistöt on yhdistetty toisiinsa kaksinkertaisella valokaapelilla. Osa työasemista on erotettu muusta verkosta omaan rinkiin ns. siltaratkaisulla, joka päästää lävitseen vain sillan toiselle puolelle tarkoitetun liikenteen. Näin liikenne nopeutuu, koska sanomien ei tarvitse aina kiertää koko verkkoa päästäkseen kohteeseensa. Aluetoimistoihin on rakennettu omat token-ring pohjaiset "pienverkot" ja ne on yhdistetty kiinteillä linjayhteyksillä suoraan Helsingin lähiverkkoon. Aluetoimistoissa on keskimäärin kolme työasemaa ja yksi palvelin. Kaikissa aluetoimistoissa on saatavilla kaikki samat lähiverkon palvelut kuin Helsingissä.

6.2
Lähiverkko

Kesällä 1991 yhdistettyjen organisaatioiden muuttaessa samaan kiinteistöön Eteläranta 6:een rakennettiin uuden lähiverkon suunnitelmien pohjalta kiinteistöön uusi lähiverkkokaapelointi sekä atk-sähkökaapelointi. Heti muuton jälkeen tietojärjestelmän muodosti yksi palvelin ja noin 30 työasemaa sekä noin 15 twinax-kaapeloinnilla IBM System 38-tietokoneeseen yhdistettyä päätettä. Lähiverkon palvelin oli 33Mhz 486 -prosessorilla varustettu IBM PS/2 90, jossa keskusmuistia oli 8 Mt ja kiintolevyä 180 Mt. Työasemat olivat prosessoritasoltaan 8086, 80286 ja 80386 -laitteita. Alussa verkkokäyttöjärjestelmänä oli IBM PC-Lan, mutta muuton yhteydessä se vaihdettiin Microsoft Lan Manageriin.

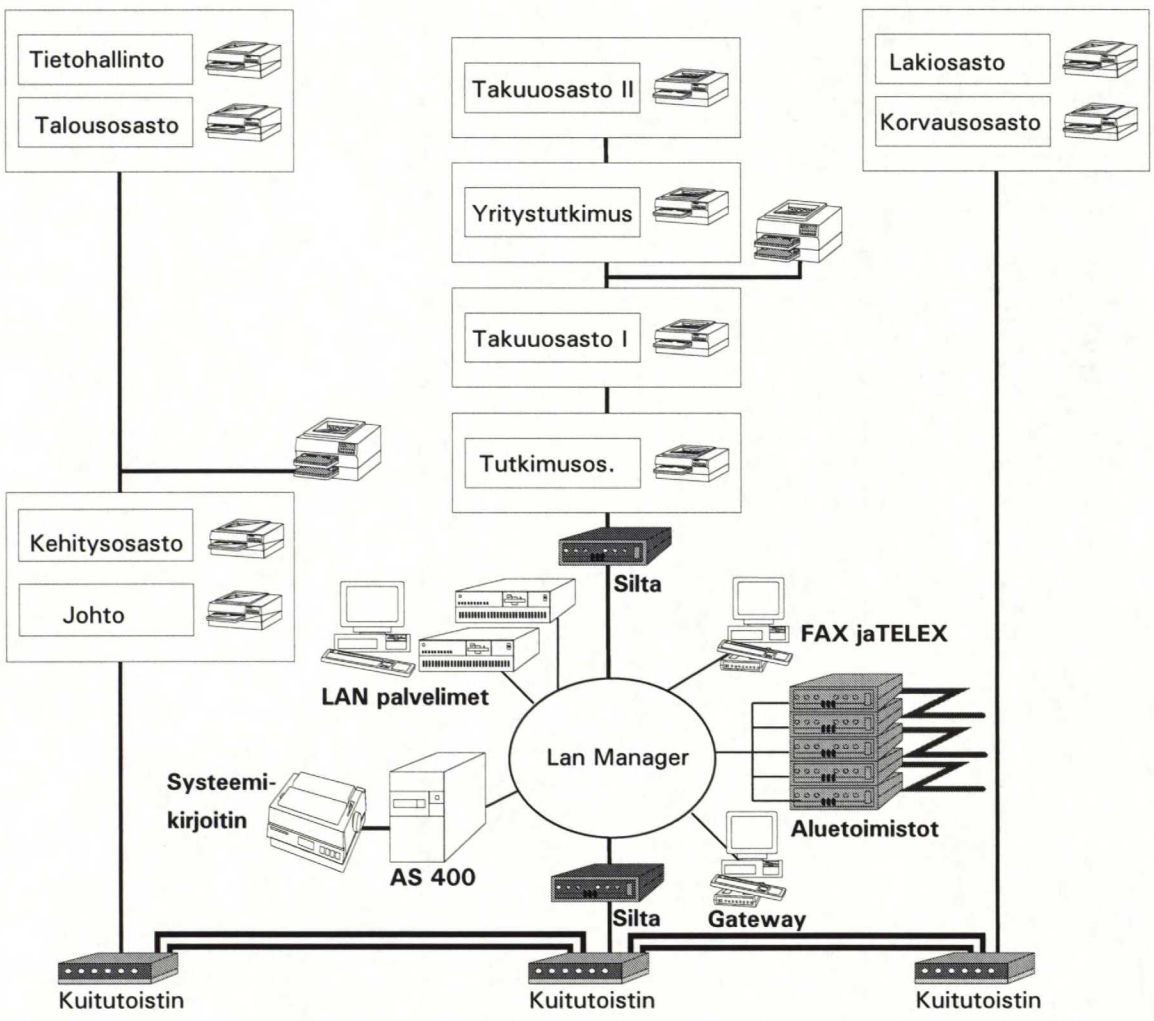
Lähiverkkoa lähdettiin kasvattamaan lisäämällä tasaisesti työasemien ja palvelimien määrää, ja siirtämällä palveluja lähiverkkoon. Ulkomaan riskien tuotantosovellus perustui perinteiseen toimistominikoneeseen ja ohjelmisto rakennettiin alunperin IBM S/38 järjestelmälle, johon yhteydenpito alunperin hoidettiin twinax-kaapeloinnilla toteutetun verkon kautta päätteillä. Twinax-kaapelointi ja päätteet poistettiin vaiheittaisesti lähiverkkoa laajennettaessa asentamalla Token-ring lähiverkon ja IBM S/38:n välille porttikone, jonka pääteohjain-emuloinnin kautta saatiin yhteys verkon työasemalta minikoneeseen. Samanaikaisten yhteyksien määrä oli rajoitettu, samoin nopeus.

Minikoneen laitteistokapasiteetin jäädessä pieneksi järjestelmä siirrettiin IBM AS400 minikoneelle, joka ominaisuuksiltaan soveltuu paremmin mikroverkkoon. As/400 minikoneeseen on kytketty suoraan oma systeemikirjoitin, jolla järjestelmän laajemmat raportit tulostetaan, osa raporteista voidaan tulostaa myös verkon laserkirjoittimille. Koneessa on myös oma nauha-asema, jolla otetaan tietokannan varmistukset. IBM S/38 porttikoneesta voitiin luopua ja yhteys muodostetaan nyt suorana istuntona työaseman 3270-pääte-emulointiohjelman avulla AS/400:aan. Windows-pohjaisen pääte-emulointiohjelman avulla myös tiedonsiirto sovelluksesta

helpottuu ja yhteys voidaan saada nyt tarvittaessa miltä tahansa työasemalta. Yhteyttä varten työasemalle on kuitenkin vielä asennettava LLC-rajapinnan tarjoavat lähiverkkoajurit sekä ajettava taustalla PCSupport 3270-työasemaohjelmistoa, joka kuluttaa työaseman käytössä olevia muistiresursseja.

Alusta alkaen on erilaisia palveluja pyritty mahdollisimman paljon siirtämään lähiverkkoon, josta ne ovat kaikkien lähiverkkoon liitettyjen työasemien saatavilla. Lähiverkon kaapelointia pitkin kulkeekin nykyisin monenlaista informaatiota: lähiverkko-ohjelmiston kutsuja, tiedostosiirtoja, tulostuksia, minikoneyhteyksiä, ulkoisia tietoliikenneyhteyksiä, fax- ja telex-sanomia jne. Verkon teoreettinen nopeus on 16 miljoonaa tavua sekunnissa, mutta käytännössä esim. tiedoston siirtonopeus työaseman levyltä palvelimelle on luokkaa 150 kilotavua/sek. eli yhden täyden 1.44 Mb levykkeellisen kopiointiin kuluu noin 10 sekuntia.

Kuvio 20 Takuukeskuksen lähiverkko



Normaalikäytössä verkko toimii vain n. 2 prosentin kuormituksella, mutta monen käyttäjän käynnistäessä yhtaikaisesti ohjelmia palvelimelta käyttöaste kasvaa rajusti. Järjestelmän rungoksi valittu IBM Token-Ring kaapelointi sekä Lan Manager Netbios-pohjainen verkkokäyttöjärjestelmä ovat mahdollistaneet sen, että verkossa on voitu liikennöidä yhtä aikaa erilaisilla protokollilla. Samoin järjestelmän nopeus ja siirtokapasiteetti on ollut riittävä, eikä verkon kuormitus jyrkästi kasvaneesta käytöstä huolimatta ole aiheuttanut ongelmia.

Palvelinkoneissa käyttöjärjestelmänä on tällä hetkellä IBM tai Microsoft OS/2 ja lähiverkko-ohjelmana Microsoft LanManager. Lähiaikoina ainakin tietokantapalvelimissa tullaan siirtymään Windows NT käyttöjärjestelmään. Palvelimia on hyvin erilaisissa tehtävissä, raskaista tietokantasovelluksista aina suhteellisen passiivisiin gateway-tyyppisiin palvelimiin. Noin kolmannes palvelimista on joko kokonaan tai osittain kirjoitinpalvelimina. Palvelimia hankittaessa on painotettu laitteen toiminnan luotettavuutta, toimittajan osaamista ja tukipalveluja. Toisinaan tämä on tarkoittanut kompromisseja laitteen tehokkuuden ja teknisen kehittyneisyyden kannalta, mutta samalla on vältytty myös suuremmilta teknisiltä ongelmilta.

Työasemien lukumäärää lisättäessä jouduttiin huomioimaan monenlaisia tarpeita. Laitekannan kehittyminen ja kasvavat vaatimukset johtivat siihen, että yhden valmistajan tuotteista ei löytynyt tarvittavia ratkaisuja ja laitehankintapolitiikkaa jouduttiin muuttamaan. Aikaisemmin tiukasti IBM:n laitteisiin tukeutuneet ratkaisut saivat nyt rinnalleen myös muiden toimittajien laitteita. Ratkaisun tiedettiin lisäävän ylläpito- ja huoltokustannuksia, mutta laitteiden hinta ja teho/laatu-suhde oli muilla toimittajilla parempi. Enää ei myöskään haluttu olla riippuvaisia vain yhden laitevalmistajan tuotteista, varsinkin kun näytti siltä, että IBM:n ja Microsoftin "tiet olivat erkanemassa".

Uusien laitteiden mukana tuli myös joitakin uusia teknisiä ongelmia, välillä jopa sellaisia, joihin ei löytynyt apua ohjelmisto- tai laitetoimittajilta, vaan ne piti ratkaista itse. Ongelmista kuitenkin selvittiin ja kokonaisuudessaan laitteistostandardin laajentaminen oli pitkällä tähtäimellä onnistunut valinta.

Uusia laitteita hankittaessa jouduttiin myös arvioimaan laitteiden käyttöikää ja teknisen kehityksen nopeutta ja suuntaa.

6.3
Verkon työasemat

Windows-käyttöliittymä, ja sitä myöten Windows-ohjelmat, ovat asettaneet suhteellisen korkean vaatimustason laitteiden suorituskyvylle. Toimivan lähiverkon ja tietojärjestelmän olisi alunperin voinut rakentaa myös DOS-pohjaisena, jolloin laitevaatimukset olisivat olleet huomattavasti pienemmät, mutta jo alusta asti tehtiin strateginen valinta graafisen käyttöliittymän ja siinä toimivien ohjelmien puolesta. Samoin kaikilta hankituilta uusilta laitteilta tai ohjelmilta on vaadittu Windows- ja verkkoyhteensopivuutta. Ratkaisu on ollut onnistunut ja tällä hetkellä sekä työasemat että ohjelmistot (käyttöliittymä ja valmisohjelmisto, toimistoautomaatiotuotteet) ovat toiminnallisesti hyvällä tasolla, ja vastaavat tämän päivän tarpeita sekä tulevaa kehitystä.

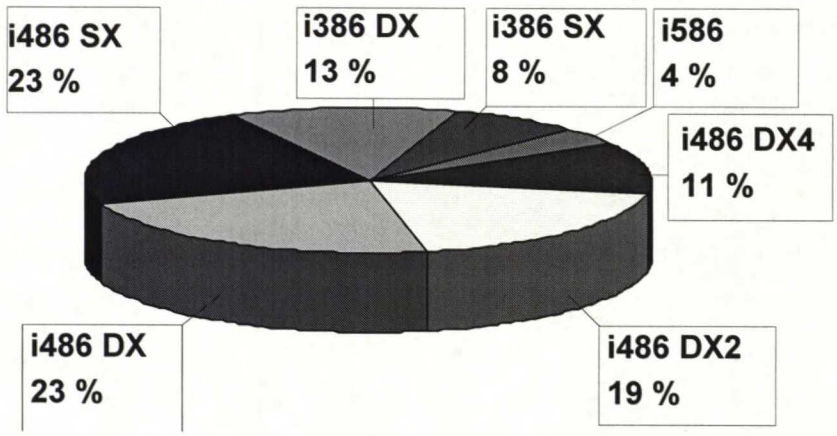
Käyttöjärjestelmänä työasemakoneissa on alusta alkaen ollut IBM tai Microsoft DOS (tällä hetkellä käytössä versio 5.0 tai uudempi). Windows-käyttöliittymä otettiin käyttöön jo heti sen ilmestyttyä Valtiontakauslaitoksen (VATA) aikoina (Windows 286). Sen sijaan Vientitakuulaitoksessa ei Windows-käyttöliittymää käytetty ja tästä syystä PC-laitteita oli vain muutama ja nekin suhteellisen pienitehoisia. Lähiverkkoa rakennettaessa on alusta alkaen pyritty hankkimaan vähintään sen hetkisen ns. "entry-level" tasoisia koneita. Tällä on pyritty takaamaan laitteille laskettu n. viiden vuoden käyttöaika, joka nykyisen laitteisto- ja ohjelmistokehityksen vauhdissa on kuitenkin melko pitkä.

Laitekantaa uusimalla ja laitteita kierrättämällä työpisteiden vaativuustason mukaan on pyritty tarjoamaan kaikille työtehtävien vaatimusten mukainen työasema. Olemassa oleva laitetaso säätelee mm. joitakin ohjelmistohankintoja ja ohjelmistopäivityksiä, esimerkiksi kaikkien käytössä olevaa tekstinkäsittelyohjelmaa ei voida päivittää uuteen versioon, jos se vaatii hyvin toimiakseen paremman laitteen kuin Takuukeskuksen käytössä oleva teholtaan huonoin työasema. Sama toimii myös päinvastoin, uusi tuotantosovellus

Windows- pohjaisessa client/server-ympäristössä vaatii yleensä myös tehokkaat työasemat,.

Käyttäjillä on nyt pääsääntöisesti käytössään 486-tason laitteet, joilla graafisen Windows-käyttöympäristön ja siinä toimivien sovellusten käyttö on mahdollista. Laitteet ovat yleisten teollisten laitestandardien mukaisia. Keskimääräisessä työasemassa on Intel 486 33 Mhz prosessori, 8 Mt keskusmuisti, 270 Mt kiintolevy, 1,44 Mt levykeasema, 14 tuuman SVGA näyttö, hiiri ja näppäimistö. Lähiverkon pääpalvelimina käytetään esim. IBM PS/2 95-AMT-koneita Intel 486DX2 tai Pentium prosessorilla. Tiedosto- ja tietokantapalvelimissa on vähintään 16 megatavua RAM-muistia ja 2 gigatavua SCSI-kiintolevyä 256 kt välimuistilla. Palvelimien kokoonpano riippuu paljon niiden tehtävistä; esim. pienen työryhmän PC-Lan kirjoitinpalvelimena toimii vielä 8086-prosessorilla varustettu IBM PC XT-laite.

Kuvio 21 Mikrotietokoneiden prosessorijakauma



Kaikki verkossa olevat laitteet saavat fyysisen yhteyden verkkoon samalla tavoin: niihin on asennettu lähiverkkosovitin, joka puolestaan on työasemakaapelilla kiinni lähiverkko- pistokkeessa. Laitetta käynnistettäessä konfigurointitiedosto lataa keskusmuistiin lähiverkon fyysisen tason ajurit, jolloin kaikki kaapelointia käyttävä tietoliikenne on mahdollista. Eri ohjelmilla, kuten lähiverkko-ohjelmalla AS/400-yhteysohjelmalla ja tietoliikenneohjelmilla

on omat tapansa lähettää ja vastaanottaa informaatiota verkossa, mutta fyysinen rajapinta on näille kaikille sama.

Työasemien ja käyttöjärjestelmien tekninen kehitys on Valtiontakuukeskuksessa suhteellisen nopeaa ja sitä on voimakkaasti ohjannut valittu ohjelmistoarkkitehtuuri. Valinta on ollut kuitenkin onnistunut ja kehityksen nähdään jatkuvan samanlaisena myös tulevaisuudessa.

6.4
Takuukeskuksen sovellusarkkitehtuuri

Sovellusohjelmia on tällä hetkellä käytössä kymmeniä erilaisia. Tekstinkäsittelyyn, taulukkolaskentaan, tilinpäätösanalysointiin, julkaisuihin jne. on käytettävissä valmiina hankittuja ohjelmistopaketteja. Erityiskohteisiin, kuten takuuvastuiden seurantaan, takaushakemusten ja -vastuiden käsittelyyn sekä korvausten käsittelyyn on käytössä räätälöidyt ohjelmistot. Sovelluskehitys oli yhdistymisen alkuvaiheessa pientä, lähinnä olemassa olevien sovellusten ylläpitoa. Ainoastaan kotimaan linjan hakemustenkäsittelysovellusta kehitettiin, koska se oli ainoa Windows ja lähiverkkoympäristöön alunperin suunniteltu sovellus. Valmisohjelmistopuolella siirryttiin vaiheittain DOS-pohjaisista sovelluksista Windows-sovelluksiin.

Molemmilla linjoilla vastuun seuranta sekä siihen liittyvä takausmaksujen laskutus on toteutettu perinteisin menetelmin mini- ja suurkoneympäristössä. Kaikki muut sovellukset toimivat MS-DOS- käyttöjärjestelmän alaisuudessa. Linjojen tuotantosovellukset eroavat olennaisesti toisistaan. Tällä hetkellä sovellusarkkitehtuuria häiritsee päällekkäisyys, eli samoja tietoja syötetään ja käsitellään useaan kertaan eri paikoissa. Molemmat vastuunseurannan sovellusympäristöt korvautunevat parin vuoden kuluttua graafiseen käyttöympäristöön yhteensopivilla ohjelmistoilla, jolloin kaikkien on mahdollisuus ajaa useampaa ohjelmaa yhtaikaa samassa koneessa moniajona, ja lisäksi helpommin vaihtaa tietoa sovellusten välillä

Ulkomaan riskin linjan TAKUULLA-sovellus on käyttäjien mielestä liian hidas ja epäluotettava, ja siinä on vanhahtava käyttöliittymä. Se ei palvele lainkaan alkuperäistä tarkoitustaan eli takuiden käsittelyä ja takuuvastuiden seurantaa. Ohjelman käyttö on hankalaa ja epäjohdonmukaista ja virhetilanteita sattuu usein.

Suuri muutos käyttäjien kannalta on ollut toimistoautomaation kehittäminen. Tekstinkäsittelyohjelman vaihto, taulukkolaskenta, sähköposti ja muut toimistotyösovellukset ovat muuttaneet työtapoja ja työtehtäviä toimistopalvelujen puolella. Kone- tai puhtaaksikirjoittajia ei enää ole ja lähes kaikki teksti- ja kuvamateriaali tuotetaan itse. Sähköiset lomakkeet ja valmiit kirjoitus- ja kuvapohjat nopeuttavat asiakirjojen luomista. Tästä seurannut teksti- ja kuvatietokantojen nopea kasvu on aiheuttanut paineita dokumenttien ja asiakirjojen hallinnalle sekä sähköiselle arkistoinnille.

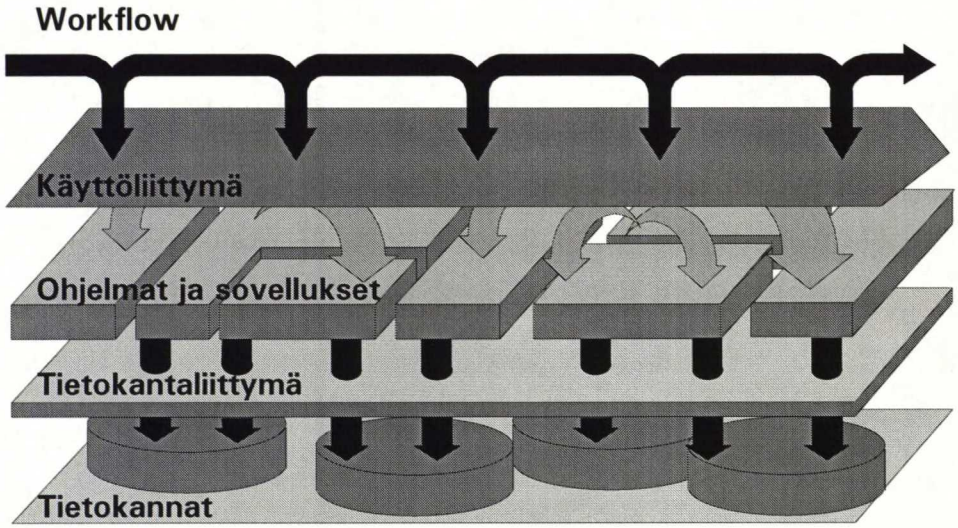
Kotimaan riskin linjalla on noudatettu alusta alkaen hajautettua tietojenkäsittelyarkkitehtuuria, joka perustuu tehokkaisiin työasemiin sekä lähiverkkoon. Kotimaan linjan järjestelmä siirrettiin lähes sellaisenaan uuteen järjestelmään, jossa sen kehittämistä jatkettiin. Kotimaan linjalla järjestelmä perustuu useamman eri ohjelmiston käyttöön, joita käytetään eri työvaiheissa.

Windows-pohjaisen hakemustenkäsittelysovelluksen rakentaminen oli alkanut jo VATA:ssa ja se jatkui edelleen Valtiontakuukeskuksessa. Osa käytettävistä ohjelmista oli ja on vieläkin DOS-pohjaisia, joista mm. tilinpäätösanalysointiin käytettävä Trennus toisinaan tuottaa ongelmia Windows-ympäristössä. Kuitenkin sovellukset on saatu sovitettua toisiinsa suhteellisen hyvin ja tiedon siirto ja kerääminen eri sovelluksista onnistuu kohtalaisen hyvin.

Sekä sovelluskehityksen että tiedonhallinnan (tietokantastandardit) puolella on kehitystyö vasta aluillaan. Tekninen infrastruktuuri on nyt saatu sellaiselle tasolle, että kehittämisen painopiste ja omat resurssit voidaan suunnata sen hyödyntämiseen tietojärjestelmäkehityksessä.

Sovellusohjelmien valinnassa keskeisinä kriteereinä ovat käyttöliittymäyhteensopivuus ja sovellusten väliset tiedonsiirto-ominaisuudet. Päällekkäisten sovellusten lukumäärää vähennetään voimakkaasti, mutta toisaalta kokonaan uusia sovellusalueita tulee jatkuvasti käyttöön.

Kuvio 22 Sovellusarkkitehtuuri



Sovellusten yhteensopivuuden vaatimus kasvaa nopeasti, mikä lisää sovellusten tiedonhallinta-, tietoliikenne- sekä käyttöliittymästandardien yhtenäistämisen tarvetta. Windows-yhteensopivien ohjelmistojen käyttöönotto on askel yhtenäisempään suuntaan. Lisäksi sovellusten toimivuus paikallisverkossa on välttämätöntä, joten hankinnat painottuvat ohjelmistojen verkkoversioihin.

Peruslähtökohtana järjestelmän hyödyntämisessä on yleisesti käytössä olevat valmisohjelmistot. Valmissovellusten pääasiallisina valintakriteereinä ovat sovelluksen yhteensopivuus tietojärjestelmään ja arkkitehtuuriin sekä sovelluksen kehitysnäkymät. Valmisohjelmistoja on yleensä tarjolla useiden eri valmistajien erilaisina versioina, joiden toiminnalliset erot toisinaan ovat hyvin pieniä. Samoin hetkellisesti saattaa esiintyä teknisesti kehittyneempiä ohjelmia, mutta yleensä kilpailijat reagoivat omilla tuotteillaan nopeasti. Tärkeämpänä on pidettävä ohjelmiston ja valmistajan toimintaluotettavuutta ja kehitysnäkymiä. Jos ohjelmistotoimittajan näkemys alan tulevasta kehityksestä on

samansuuntainen kuin organisaation tietojärjestelmien kehittäjillä, voidaan olettaa tuotteen sopivan sovellusarkkitehtuurin puitteisiin myös tulevaisuudessa.

Räätälöidyt tai tilaustyönä tehdyt (itse tai ulkopuolisilla teetetyt) ohjelmat tulevat yleensä tuotantotoiminnan tiettyyn tarpeeseen tai korvaamaan vanhaa tuotantosovellusta. Näitä sovelluksia hankittaessa pääpaino asettuu sovellusarkkitehtuurin ja tietohallintastrategian tuomiin puitteisiin. Toimittaja valitaan erikseen kuhunkin projektiin, mutta sovellukselle asetetut laatu- ja toimintakriteerit pysyvät suhteellisen samanlaisina. Oletusarvona tilattavan sovelluksen tulee täyttää samat kriteerit kuin valmisohjelmat.

Eri osastoilla sovellusten itsenäinen käyttö lisääntyy. Sovellusten hankinta koordinoidaan edelleen keskitetysti, jotta standardinmukaisuus säilyy. Erilaisten sovellusohjelmien käyttö laajenee kaikille Takuukeskuksen strategisille, taktisille ja operatiivisille toimintojen alueille.

Keskeinen merkitys tulee olemaan yhtenäisellä käyttöliittymällä, joka madaltaa käyttökynnystä ja mahdollistaa moniajon. Tärkeää on myös joustava sovellusten välinen tiedonsiirto sekä kyky käyttää sovelluksesta riippumatta samoja tietokantoja.

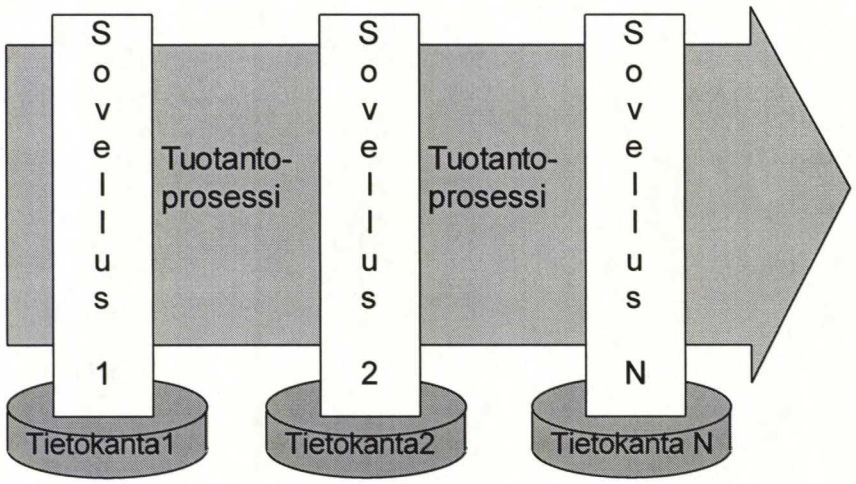
Uudet sovellukset muuttavat työntekijöiden totuttuja työskentelymetodeja ja apuvälineitä sekä organisaation työnjakoa. Eniten uusien sovellusten käyttöönottoa hidastavat inhimilliset ja sosiaaliset tekijät.

6.5
Tiedonhallinta ja tietovarastot

Molemmilla linjoilla tiedonhallinta on perustunut sovelluskohtaisiin tietokantoihin ja tiedostoihin. Takuukeskuksessa on käytössä useita erilaisia tietokantoja eri tarkoituksiin, ja ne kommunikoivat huonosti keskenään. Samaa tietoa saatetaan syöttää useaan eri tietokantaan.

Tiedonhallinnassa ollaan laajamittaisen kehitystyön edessä. Käytössä on useita erilaista tietokantoja ja -standardeja. Nämä eivät toistaiseksi keskustele keskenään, jolloin samaa tietoa joudutaan kirjaamaan moniin eri paikkoihin. Kehitystyössä yhtenä tärkeimmistä asioista nähdään tietokantojen yhtenäistäminen moderniin, avoimeen arkkitehtuuriin yhteensopivaksi. Tavoitestandardeina tietokantojen hallinnassa ovat olleet mm. relaatiomalli ja SQL-kyselykieli.

Kuvio 23 Sovellusten tietokannat



Sovellusten tietokannat

TOIMINTO	TIETOKANTA
Vastuunseuranta	Takuulla, DMS
Korvaus	Midec
Kotim.riski,hak.käsittely	Omnis5
Ennuste, seuranta	Trennus, Trandat
Taloushallinto	Focus/Postipankki
Siirt.saat.perintä	K-mies
Palkanlaskenta	Tukiset

Tekstitietokannat

Tekstinkäsittelytiedostot talletetaan joko tiedostopalvelimelle, käyttäjien mikrotietokoneiden kiintolevyille tai erillisille levykkeille. Yhtenäistä nimeämisohjetta tai tekstitietokannan hallintaohjelmaa ei ole käytössä.

Kuvatietokannat

Tuotannolliset valmiskuva-arkistot ovat toistaiseksi manuaalisia (velkakirjat, sopimukset, tositteet ym.). Osa muuhun tarkoitukseen tuotetuista tai talletetuista kuvista tai esitysgrafiikasta talletetaan samoin kuin tekstinkäsittelytiedostot. Tukitoiminnoissa kuvia ja julkaisuja tehdään itse eri tarkoituksiin mm. PageMakerilla, Harvard Graphicsilla, Windows Paintbrushilla sekä Lotuksella ja Excelillä. Näillä tuotetut kuvat on talletettu epäjärjestelmällisesti käyttäjien omille levykkeille ja kiintolevyille sekä tiedostopalvelimelle.

Ulkoiset tietovarastot

Maatutkimus, takuuosastot, yritystutkimus sekä laki- ja korvausosastot käyttävät jatkuvasti ulkoisia tietopankkeja toiminnassaan. Ulkoisten tietovarastojen käyttö laajenee uusille alueille sekä tietohakujen lukumäärä kasvaa koko ajan.

Päätearkisto

Päätearkisto on valtion arkistointiohjesäännön mukainen manuaalinen arkisto.

6.6
Tietoliikenne

Erilaisia tietoliikennepalveluja on ollut käytössä jo pitempään kaikilla osastoilla. Tietoliikenteen avulla on mahdollista saavuttaa merkittäviä aika- ja kustannussäästöjä käsittelyprosessien eri osa-alueilla. FAX- ja telex-palveluiden liittäminen lähiverkon osaksi mahdollistaa telekopioiden lähetykset ja vastaanoton kaikilta työasemilta ja poistaa useita turhia työvaiheita. Sisäinen sähköposti ja sen liittymät ulkoisiin sähköposteihin nopeuttaa huomattavasti tiedonkulkua ja parantaa työtehoa. Tietoliikenneyhteyksien kautta saadaan

myös paljon informaatiota luotettavasti ja nopeasti. Käytetyimpiä ovat ulko- ja kotimaiset luottotiedot sekä asiakastiedot sekä ulkoinen sähköposti. Samoin sähköistä viestintää käytetään yhteydenpidossa Valtiontakuukeskuksen ulkomaisiin sidosryhmiin mm. Bernin Unioniin ja OECD:en.

Tietoliikenteen kehittäminen ja sen tarjoamat uudet mahdollisuudet nähdäänkin Valtiontakuukeskuksessa eräänä tärkeänä mahdollisuutena kehittää tietojärjestelmää ja organisaation toimintaa tulevaisuudessa. Tietoliikennestrategiassa pyritään huomioimaan liiketoiminnan tarpeet ja muutokset, määrittämään nykyinen asema ja luomaan tavoitteet tulevaisuuteen sekä määrittämään keinot, joilla asetetut tavoitteet saavutetaan.

Ulkoisten yhteyksien kehittämisessä tavoitteina on tiedonhankinnan tehostaminen, monipuolistaminen ja nopeuttaminen sekä tiedon- ja informaationvälityksen parantaminen. Tietopankkipalvelut saatetaan verkon avulla kaikkien käyttöön ja pyritään integroimaan ulkopuoliset tietopalvelut omaan tuotantoprosessiin. Tämä tapahtuu täydentämällä teknisiä valmiuksia ja kouluttamalla vastuuhenkilöt osastojen tiedonhankintaan. Olemassa olevia tietopalveluiden käyttöä tehostetaan ja uusia tietopankkipalveluita seurataan ja kokeillaan. Ulkoiset sähköpostiyhteydet ja palveluverkot tuovat omat lisäarvonsa tietoliikenteelle ja myös niitä pyritään hyödyntämään organisaation toiminnassa.

Tällä hetkellä ulkoiset yhteydet hoituvat pääosin a) oman X.25 yhdyskäytävän avulla, jonka kautta voidaan olla yhteydessä kaikkiin tarvittaviin ulkoisiin palveluihin, b) erilaisten gateway-koneiden ja palvelujen avulla kiinteillä yhteyksillä sekä c) lähiverkon kautta käytettävissä olevan modeemipoolin kautta valinnaisiin soittosarjoihin. Ulkoisessa sähköpostiyhteydessä X.400 sanomanvälitysstandardi tulee kyseeseen sekä kotimaisessa että kansainvälisessä sanomanvälityksessä. Valtiontakuukeskuksessa X.400-sähköposti on integroitu sisäiseen sähköpostiin ja otettiin virallisesti käyttöön 1994 vuoden lopulla. Koekäytössä X.400 on ollut vuoden 1994 alusta alkaen.

X.400:n puitteissa yhteistyötä ollaan kehittämässä muutamien Valtiontakuukeskuksen sidosryhmien ja yhteistyökumppanien kanssa.

Organisaation sisäisen tietoliikenteen nähdään muodostuvan seuraavista osa-alueista:

- sähköposti ja sisäinen tiedotus
- yhteiset tietokannat
- sovellusten välinen tietoliikenne
- yhteydet aluetoimistoihin paikallisverkon kautta
- etäyhteydet (kotitoimistot, kannetavat yms)

Sisäisen tietoliikenteen kehittäminen jakaantuu tämän mukaan kolmeen eri osa-alueeseen:

- sisäisen tiedonkulun parantaminen
- sovellusten välinen tiedonsiirto
- mobile office-konsepti

Lyhyenä yhteenvetona Valtiontakuukeskuksen tietoliikenne koostuu tällä hetkellä seuraavista osa-alueista ja tuotteista:

Sisäinen sähköposti

VTK:n sisäinen sähköpostiohjelmisto on Microsoft MS-Mail 3.2. Otettu käyttöön alkukesästä 1993.

Ulkoiset sähköpostiyhteydet

VTK:lla on oma Elisa-sähköpostitunnus, mutta pääasiallisena ulkoisena sähköpostina on käytössä X.400-yhteys. X.400 on integroitu sisäiseen sähköpostiin ja kaikilla käyttäjillä on oma X.400-osoite sekä mahdollisuus lähettää tai vastaanottaa X.400-viestejä suoraan MS Mail -sähköpostiohjelmasta. (Gateway tuotteet: Eicon X.25 OSI LanGateway ja MS Mail Gateway to X.400).

OECD ja Bernin Unionin sähköpostiyhteydet on käytössä kansainvälinen taloustutkimus-osastolla. Nämä yhteydet toimivat tällä hetkellä perinteisesti työasemamodeemilla (yhteys PADiin /Datapak/X.28), johtuen näiden yhteyksien vaatimista erikoisohjelmistoista.

Fax, Telex & EPL

Alcomin LanFax (fax) ja Softlinen Fax (fax, telex, epl) ovat käytettävissä kaikista lähiverkon työasemista. Fax-lähetys suoraan tekstinkäsittelyohjelmasta, vastaanotto keskitetty; router-henkilö jakelee saapuneet faxit (esim MS Mail:n avulla).

Tietopankkiyhteydet

Tietopankkiyhteyksiä varten on VTK:lle eri osastoille räätälöity oma helppokäyttöinen käyttöliittymä, jonka avulla yhteydet tietopankkeihin saadaan mistä tahansa verkossa olevasta työasemasta. Procomm+ for Windowsilla tehdyn käyttöliittymän avulla saadaan yhteys haluttuun tietopalveluun yhdellä napinpainalluksella. Käyttöliittymä mahdollistaa Windowsin tarjoamien palvelujen täysimittaisen hyödyntämisen. Tietopalveluihin kuuluu erilaiset tietopankit sekä koti- että ulkomailla (pääosin asiakas- ja luottotiedot, yritystiedot yms.). Yhteys muodostetaan joko verkkomodeemin (modeemipooli Async.Gateway) tai X.25-palvelimen kautta (pakettiverkko XPAD / Eicon X.25 Gateway).

BusinessInfotel

VTK:lle räätälöity oma käyttöliittymä. Pääsy erilaisiin tietopankkeihin ja palveluihin (mm. VTKK tietokannat, pankkipalvelut yms.) sekä modeemin että pakettiverkon kautta.

Telesampo

Oma käyttäjätunnus. Yli sata eri osapuolten tuottamaa tietopalvelua.

Etäkäyttöyhteydet

Etäkäyttöpalvelimen avulla VTK:n lähiverkon resurssit (tiedosto-, tulostin-, tietokanta-, tietoliikenne-, sähköpostipalvelimia jne.) saadaan etätyöasemien

käyttöön. Etäistyöasemana voi toimia mikä tahansa PC-yhteensopiva mikro (esim kannettava mikro ja käsipuhelin tai PC-kotimikro + modeemi), jossa on tarvittava etäkäyttövarustus.

Aluetoimistot

VTK:n aluetoimistot on yhdistetty LanWay palvelun avulla suoraan Helsingin toimiston lähiverkkoon (Andrew 7404 sillat, nopeus 64 kb/s). Kukin aluetoimisto muodostaa oman fyysisen renkaan.

Lähiverkko

Token Ring IBM type 1 (STP) kaapelointi, LanManager 2.2 verkkokäyttöjärjestelmä (Netbios/NetBEUI, AS/400 LLC-rajapinta). n. 150 työasemaa ja n. 30 erilaista palvelinkonetta (gatewayt, ohjelmisto- ja tiedostopalvelimet, kirjoitinpalvelimet, tietokantapalvelimet, AS/400 jne). Kolme paikallista rengasta sekä viisi aluetoimistoyhteyttä (sillat).

7
VALTIONTAKUUKESKUKSEN TIETOTURVAN TAVOITTEET JA KOHTEET

Liiketoiminnan ja tietojenkäsittelyn strategioiden pohjalta määritetyn tietoturvapolitiikan tulee tukea samoja päämääriä ja tavoitteita, joita tietojärjestelmälle on asetettu. Tietojenkäsittelyn arkkitehtuurimäärityksen pohjalta on valittava sellaisia ratkaisuja, joissa tietoturvan eri osa-alueet tulevat huomioiduksi sekä tietojärjestelmän kehittämisen että toteuttamisen ja käytön aikana.

7.1
Tietoturvan tavoitteet

Valtiontakuukeskuksessa tietojärjestelmälle ja sen kehittämiselle asetetut tavoitteet voidaan tiivistää seuraavasti:

⇒ tiedon yhteiskäyttöisyys

⇒ reaaliaikaisuus

⇒ luotettavuus

⇒ palvelevuus

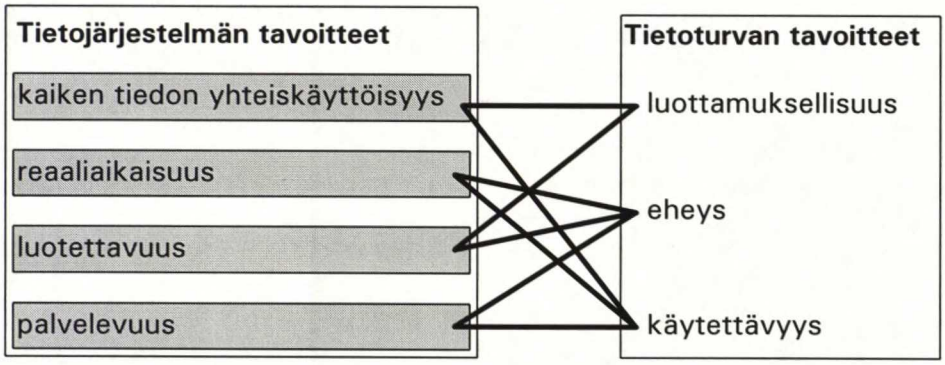
Näitä tavoitteita tarkasteltaessa tietoturvan kannalta, voidaan huomata niiden vastaavan tietoturvan kannalta tiedon kolmea ominaisuuttaa: luottamuksellisuus, eheys ja käytettävyys.

Luottamuksellisuus; tiedot ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä paljasteta tai saateta asiaankulumattomien käyttöön.

Eheys; tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ne ole laitteisto- tai ohjelmistovikojen, katastrofien tai tahallisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

Käytettävyys; järjestelmien tiedot ja palvelut ovat tarvittaessa niihin oikeutettujen käytettävissä.

Kuvio 24 Tietoturvan tavoitteet ja tietojärjestelmän tavoitteet



Järjestelmän tietoturvan parantamiseksi tulisi varmistaa seuraavien tavoitteiden toteutuminen:

- tuotannon keskeytymättömyyden varmistaminen
- tietojenkäsittelystä riippuvan laadun ylläpitäminen

- tietojenkäsittelyn tehokkuuden ylläpitäminen
- tietojenkäsittelyn virheettömyyden ja häiriöttömyyden varmistaminen
- valmius jatkaa toimintaa keskeytystenkin sattuessa
- kaiken tiedon käytettävyys, luotettavuus, eheys ja oikeellisuus

Tietoturvan tavoitteiden saavuttamisen kautta parantuneen tietoturvallisuuden tuloksina edistetään organisaation toiminnan luotettavuutta ja yrityskuvan säilyttämistä, kilpailukyvyn varmistamista tietojenkäsittelyn tehokkuuden ylläpitämisen avulla.

7.2
Tietoturvakohteet ja -toimenpiteet

Tietoturvan tavoitteiden ja tietojärjestelmän tavoitteiden määrittämisen jälkeen voidaan tietoturvan kohteita ja toimenpiteitä etsiä tietojenkäsittelyn kehittämiselle asetettujen tavoitteiden saavuttamiseksi esitettyjen toimenpiteiden pohjalta.

Valtiontakuukeskuksen tietojärjestelmien kehittämiseen kuuluvat tietohallintostrategian ja Valtiontakuukeskuksen tietojenkäsittelyn kokonaistutkimuksen perusteella mm. seuraavat toimenpiteet:

- tietokantojen tekninen integrointi
- sovellusten yhtenäistäminen
- sovellusten välinen tiedonsiirto
- tietosisällön luotettavuuden parantaminen
- ylläpidon yksinkertaistaminen
- käyttöliittymän ja raportoinnin kehittäminen
- vastuuhenkilöt tietokantojen luomiseen, ylläpitämiseen ja käytön opastamiseen.
- käytettävien ohjelmistojen ja tallennustyyppien määrän minimointi
- tietoliikenteen kehittäminen

Tietoturvan kannalta tarkasteltuna näistä toimenpiteistä voidaan löytää seuraavat tietoturvan kohteet:

1. fyysinen turvallisuus ja laitteiston suojaaminen
2. sovellusten turvallisuus
3. tietojen suojaaminen
4. henkilöstöturvallisuus
5. tietoliikenteen suojaaminen

Laitekanta Valtiontakuukeskuksessa on hyvä, ja henkilökunnan asenne automaattista tietojenkäsittelyä kohtaan on melko myönteinen. Atk:n kehittämistä kohtaan on syntynyt myönteinen ilmapiiri. Ongelmana pidetään joissain tapauksissa käyttöasteen alhaisuutta sekä koulutusresurssien pienuutta.

Molemmilla linjoilla vastuunseuranta sekä siihen liittyvä takausmaksujen laskutus on toteutettu perinteisin menetelmin mini- ja isokoneympäristössä. Kaikki muut sovellukset toimivat DOS / Windows- käyttöjärjestelmän alaisuudessa. Mikrotietokonesovellusten osalta yhteensopivuus on hyvä, mutta vastuun seurantasovellukset eroavat olennaisesti toisistaan. Tällä hetkellä sovellusarkkitehtuuria häiritsee päällekkäisyys, eli samoja tietoja syötetään ja käsitellään useaan kertaan eri paikoissa.

7.2.1
Fyysinen turvallisuus ja laitteiston suojaaminen

Mikrotietokoneet ja oheislaitteet eivät vaadi erityisiä jäähdytys- tai ilmastointilaitteita tai muita erityisiä atk-tiloja, vaan ne toimivat normaaleissa toimistotiloissa. Laitteiston suojelu tulipalolta, vesivahingoilta ja muilta vastaavilta fyysisiltä vahingoilta tapahtuu suurelta osin kiinteistön ja muun irtaimiston normaalin suojelun puitteissa.

Tietoverkkoon kytkettyjen päätteiden, mikrotietokoneiden ja laitteiden lukumäärän suuruus sekä niiden sijainti kaikkialla yrityksen toimitiloissa

korostaa kulunvalvonnan merkitystä hajautetun järjestelmän suojauksessa. Kulunvalvonnalla on varmistettava asiattomien pääsyn estäminen yrityksen toimitiloihin ja , että vieraitten (esim. asiakkaiden ja huoltohenkilöiden) liikkumista yrityksen tiloissa valvotaan. Tähän voidaan vaikuttaa esim. oviin asennetuilla sähkölukoilla, jotka voidaan avata vain pääsyyn oikeuttavalla kortilla ja/tai koodilla.

Kulunvalvonnan tulisi huolehtia seuraavista seikoista:

- vierailijoiden saapumis- ja lähtöaika sekä vieraasta yrityksen sisällä vastaava henkilö kirjataan vastaanottotiloissa muistiin
- vierailijoille jaetaan vierailija-kortti
- asiakastiloihin ei asenneta atk-laitteita, jotka mahdollistavat pääsyn yrityksen tietojärjestelmään
- asiakastiloista ei pääse suoraan yrityksen varsinaisiin toimitiloihin
- muualla, kuin asiakastiloissa, ei vieraita saa jättää yksin

Laitteiston toiminnan seuraamiseksi ja ylläpidon helpottamiseksi yrityksessä on oltava laitekirjasto. Laitekirjastoon merkitään kaikki yrityksessä olevat atk-laitteet (mikrotietokoneet, kirjoittimet, modeemit jne.). Laitekirjastosta on käytävä ilmi ainakin laitteen malli ja kokoonpano, laitetoimittaja / huolto, laitteen sijoituspaikka yrityksessä ja käyttäjä. Samoin laitekirjastoon voidaan merkitä laitteen toiminnassa esiintyneet häiriöt ja mahdolliset korjaukset tai varaosat.

7.2.2
Ohjelmistojen ja tietojen suojaus

Palvelinkoneiden ja yhteiskäyttöisten tietojen ja tietokantojen sekä ohjelmistojen suojausta varten on nimettävä vastuuhenkilöt. Henkilöt voidaan nimetä esim. osasto-, tietokanta- tai konekohtaisesti. Lähiverkko-ohjelmistoon kullekin käyttäjälle on määrättävä tunnus ja salasana sekä määriteltävä hänen käytössään olevat resurssit päivitysoikeuksineen. Tiedon oikeellisuus turvataan minimoimalla erilliset talletusvaiheet ja määrittelemällä henkilökohtaiset vastuualueet.

Tärkeimpänä tietojen suojausrutiinina on tiedostojen varmuuskopiointi. Varmuuskopiointi on suunniteltava ja ohjeistettava siten, että se tapahtuu helposti ja nopeasti. Yhteiskäyttöisten tiedostojen, ohjelmien tietokantojen varmistus tapahtuu parhaiten keskitetysti verkkopalvelimeen kytketyn nauhavarmistusaseman kautta. Henkilökohtaisten tietokoneiden kiintolevylle talletettujen tietojen varmistus on käyttäjän omalla vastuulla. Varmuuskopioiden otto on ohjeistettava ja käyttäjät koulutettava. Kiintolevyille asennettavat ohjelmat ja talletettavat tiedot on suunniteltava etukäteen ja dokumentoitava tarkoin ("vähin tarpeellinen"-periaate). Hakemistojen nimet ja hakemistopuun rakenne standardoitava läpi koko järjestelmän. Koko järjestelmän varmuuskopiot tulee säilyttää niille erikseen varatussa tietovälinearkistossa. Myös käyttäjillä tulee olla henkilökohtaisia varmuuskopioitansa varten oma säilytyskotelo.

Myös yksittäisten sovellusten tai tietokantaohjelmistojen ominaisuuksiin tulisi sisältyä erilaisia välineitä tietojen suojaamiseen. Tällaisia ominaisuuksia ovat mm. ohjelman sisäiset datatiedostojen varmuuskopioinnit, ohjelma-ajojen lokitiedostot, tietokannan toipuminen ja eri käyttäjätasojen- ja oikeuksien määrittelymahdollisuus.

Ohjelmistojen versionhallinta ja päivitykset sekä käytettävien sovellusten varmuuskopioiden ylläpito ja säilyttäminen kuulu atk-osaston vastuualueeseen. Organisaatiossa käytettävistä ohjelmista on tehtävä ohjelmakirjasto, josta selviää ainakin järjestelmässä käytettävät ohjelmat ja niiden versiot, mihin niitä on asennettu ja ketkä niitä käyttävät. Ohjelmakirjasto voidaan yhdistää laitekirjastoon, jos tiedot pystytään erittelemään riittävän hyvin.

Käyttöjärjestelmätasolla tietoturvaominaisuudet vaihtelevat huomattavasti. Työasemien käyttöjärjestelmät eivät tue tietoturvaa kovinkaan hyvin, sen sijaan moniajojärjestelmät sisältävät yleensä myös joitakin tietoturvapiirteitä. Palvelinten käyttöjärjestelmät ja lähiverkon käyttöjärjestelmä ovat kriittisimmät ja niissä ohjelmistojen tulisi tukea eri suojaustasoja niin yksittäisen palvelimen kuin koko verkon hallintaan. Ohjelmistoja valittaessa olisi niiden

tietoturvaominaisuuksien oltava eräs tärkeimmistä valintakriteereistä. Ohjelmatiedostoihin pääsy sallitaan vain tarkoin rajatulle ryhmälle ja erilaiset oikeudet (luku-, käyttö-, muutos-, päivitys- ja tuhoamisoikeus) on määritettävä käyttäjä kohtaisesti. Ohjelmistojen toimintaa ja palvelujen käyttöä on jatkuvasti tarkkailtava ja toiminnoista on kerättävä tiedot lokitiedostoihin.

7.2.3
Henkilöresurssien varmistaminen

Henkilöstö on yrityksen keskeisin resurssi riskienhallinnankin näkökulmasta. Se muodostaa toisaalta atk-ympäristössä kriittisen osaamisen ja rikollisen toiminnan mahdollisuudet, mutta se on myös riskienhallinnan tärkein resurssi. Henkilöresurssien varmistaminen koskee koko organisaation henkilökuntaa, mutta varsinkin organisaation toiminnan kannalta avainasemassa olevia työntekijöitä. Atk:n loppukäyttäjien kannalta riskit ovat samanlaisia kuin atk-ammattilaisten näkökulmalta, tosin atk-henkilöiden yksittäinen merkitys on suurempi. Kuitenkin myös loppukäyttäjien osaaminen, organisaatioon sitoutuminen, motivointi ja koulutus ovat merkittävässä roolissa tietojärjestelmän turvaamisessa.

Henkilöstöresursseja voidaan tarkastella seuraavien kohtien mukaisesti:[49]

1. osaaminen / osaamattomuus
2. avainhenkilöt
3. dokumentointi
4. motivointi /henkilöstön vaihtuvuus
5. rikollisuus
6. rekrytointi

1. Osaamattomuus

Atk-toiminnan strategisen osaamattomuuden seuraukset saattavat aiheuttaa yritykselle erittäin suuret taloudelliset menetykset. Tätä riskiä on lisännyt

---

[49] Pohjola s. 24

yritysten suuri atk-toiminnan johtajien tarve. Seurauksena on syntynyt tilanne, että henkilöitä, joilla ei ole johtamiskokemusta eikä tietojenkäsittelyn osaamista, on päässyt tehtävään, jonka asettamat vaatimukset ovat kykyihin nähden liian suuret. Yrityksen johdon kannalta tämän tekee kriittiseksi vielä se, että atk-toiminnan strategisen suunnittelun riskit toteutuvat vasta usean vuoden jälkeen ja niiden korjaaminenkin vie useamman vuoden.

Projektipäälliköiden ja järjestelmäsuunnittelijoiden osaamattomuus heijastuu tietojärjestelmien valmistumisen viivästymisenä sekä tuottaa järjestelmiä, jotka eivät vastaa suunniteltuja tavoitteita. Kustannukset saattavat olla huomattavat. Riskit on poistettavissa vain varmistamalla, että henkilövalinnassa saadaan sellainen ammattilainen kuin todella on tarkoituskin.

Käyttäjien osaamattomuus näkyy järjestelmän hyödyntämisessä ja sen kyvyssä tukea organisaation toimintaa. Ohjelmisto- ja laiteinvestoinnit saattavat mennä hukkaan mikäli käyttäjiä ei kouluteta käyttämään järjestelmää. Koska kouluttaminen on kallista, olisi jo rekrytointivaiheessa otettava kantaa tehtävän vaatimaan atk-osaamisen tasoon. Osaamattomat käyttäjät lisäävät järjestelmän virhe- ja ongelmatilanteita, sekä vaarantavat järjestelmän tuottaman tiedon ja informaation oikeellisuuden.

2. Avainhenkilöt

Avainhenkilöriskien syntyminen atk-yksiköissä tapahtuu yleensä verraten hitaasti. Yrityksessä pitkään toimineille henkilöille kasaantuu tietoa ja osaamista heidän hoitamistaan järjestelmistä. Tämä riski kasvaa ilman että yritys tai kyseinen henkilö sitä haluaisi. Riskin merkittävyyttä lisää heikko dokumentointi. Toimivalla varamiesjärjestelmällä voidaan riskiä pienentää. Atk-henkilöstön, kuten muunkin henkilöstön, lakko on merkittävä riski. Tämä kuten mikä tahansa muukin yrityksen avainhenkilöryhmän lakko lamauttaa varsin pian yrityksen koko toiminnan. Tätä riskiä voidaan pienentää työehtosopimusjärjestelyjen lisäksi pyrkimällä käyttötoiminnan automatisointiin.

3. Dokumentointi

Käytännössä dokumentointi on heikkoa lähes kaikissa yrityksissä. Näyttää siltä, että erillisten paperidokumenttien syntyminen ja niiden ajan tasalla pitäminen sovellutusten vanhetessa on lähes mahdotonta. Käyttämällä koneellista dokumentointia yhdistettynä itse suunnittelu- ja ohjelmointityöhön päästään ehkä parhaimpaan lopputulokseen. Tällöin henkilön poisjäänti töistä tai siirtyminen toisen yrityksen palvelukseen ei merkittävästi vaikeuta jatkotoimintaa.

4. Motivointi / henkilöstön vaihtuvuus

Henkilöstön toimenvaihtoalttiutta voidaan pienentää motivoinnin ja henkilövakuutusten avulla, mutta nekään eivät poista henkilön poisjäämistä onnettomuuden tai muun vahingon vuoksi. Korkea palkka ei sovellu ainoaksi motivoijaksi, mutta huono palkka varmaksi keinoksi lisätä toimenvaihtoalttiutta.

Atk-ammattilaisten suuri kysyntä luo mahdollisuudet paikanvaihdolle. Heikko motivaatio, suuri työpaine ja suhteessa muita heikompi palkka vaikuttavat lähtökynnykseen. Lähtevän mukana saattaa kilpailevalle yritykselle siirtyä tietoa ja osaamista, jolla on haitallinen vaikutus omaan liiketoimintaan. Muina haittavaikutuksina saattaa seurata sovellutuksen ylläpito- ja käyttövaikeudet ja mahdollisesti asiakkaille asti menevät virheet. Yleensä myös tietojärjestelmien rakentamistyö hidastuu. Hyvä dokumentointi, tietojärjestelmien strukturointi ja taiturointien välttäminen pienentävät riskiä.

5. Alttius rikollisiin toimiin

Sovelluksista vastuussa olevat henkilöt tuntevat varsin hyvin paitsi itse atk-järjestelmän niin myös sovellukseen liittyvät manuaaliset järjestelmät. Rikolliselle toiminnalle tämä tietous antaa jonkin verran paremmat onnistumismahdollisuudet. Vaikka rikollisuuden merkitystä ei olekaan syytä liioitella, on atk-ammattilaisia ja kokeneita käyttäjiä jo niin suuri joukko, että

suurten lukujen lakien mukaan tähän joukkoon saattaa kuulua myös rikoksiin alttiita.

6. Rekrytointi

Henkilöstön rekrytointivaihe on ehkä tärkein hetki pienennettäessä henkilöstöriskejä. Todellisten henkilötaustojen tarkistaminen on hyvin tärkeää. Virkatodistuksesta nähdään mahdolliset nimenmuutokset ja haastattelussa voidaan pyrkiä selvittämään syyt niihin. Tietyissä tapauksissa on mahdollista saada viranomaisilta vastaus, soveltuuko kyseinen henkilö tähän tehtävään. Henkilöstön atk-osaaminen on helpointa varmistaa valitsemalla tehtäviin henkilöt, joilla on myös riittävä atk-tuntemus. Käyttäjillä tulisi olla työtehtävän vaatima osaamistaso jo aloitettaessa, sillä atk-käytön kouluttaminen muiden työtehtävien opettelun ohessa on kallista ja aikaavievää. Samoin osaamattomat käyttäjät lisäävät atk-kustannuksia.

Henkilöstöriskien hallinnassa suuri osa ennaltaehkäisevistä toimista on normaaliin johtamistaitoon liittyviä kysymyksiä. Atk-henkilöstössä tämän johtamisen osaaminen vain korostuu; johtamistaidon osaamattomuus heijastuu paitsi hidastuneena sovellutuksien valmistumisena, huonona laatuna niin myös kasvavana tahattomien riskien todennäköisyytenä sekä rikollisen toiminnan mahdollisuuksien lisääntymisenä.

7.2.4

Tiedonsiirron suojaus

Tutkimusten mukaan organisaatioissa sisäisen ja ulkoisen tietoliikenteen kehittymien tehostaa muita atk-palveluita enemmän organisaation toimintaa sekä parantaa palvelua. Kun tietoliikenneyhteydet toimivat asiakkaalle saakka siten, että palvelut ovat saatavilla asiakkaan omilla työasemilla tietoliikenne muuttuu tärkeäksi strategiseksi kilpailutekijäksi (vrt. pankkiautomaattiverkko, kotipankkipalvelut).

Tästä näkökulmasta tulevaisuudessa Takuukeskuksen tietoturvan kannalta kriittinen kohde on tiedonsiirto. Hajautetussa järjestelmässä, jossa laitteet, sovellukset ja tietokannat ovat yhteiskäyttöisiä, tiedonsiirron toimiminen on koko järjestelmän kannalta elintärkeää. Ulkoiset yhteydet lisäävät organisaation ulkopuolelta tulevia riskejä, kuten salakuuntelu, sanomien sieppaus tai järjestelmään tunkeutuminen.

Ulkoisten riskien hallittavuutta vaikeuttaa se, että salaus- ja suojaustoimenpiteistä on sovittava toisen organisaation kanssa. Yhteyksien turvaaminen vaati niiden toiminnan ja käytön jatkuvaa valvontaa; mitä enemmän ja mitä tärkeämpiä yhteydet ovat, sitä enemmän ne kuluttavat tietoturvaan ohjattuja resursseja.

Tiedonsiirron turvallisuuden suunnittelun perustaksi on selvitettävä järjestelmän toiminnan riippuvuus tiedonsiirrosta ja tietoliikenneyhteyksistä. Selvityksen perusteella voidaan määritellä järjestelmän tiedonsiirto- ja tietoliikennehäiriöiden sietokyky. Luokitus voidaan tehdä esim. häiriöiden tai katkosten keston vaikutuksesta järjestelmän toimintaan. Suunnittelussa on huomioitava halutun järjestelmän suojauksen tason mukaisesti siirrettävän tiedon salaisuusaste, tietoliikenteen häiriöttömyys, tiedon muuttumattomuus ja varasiirtotiet.

Valinnaisia puhelinverkkoja voidaan käyttää julkisten tietojen välittämiseen ja tilapäisesti varajärjestelmänä. Puhelinverkko ei tarjoa varmoja menettelyjä luvattomien tunkeutumisyritysten estämiseksi. Suojautuminen edellyttää käyttöoikeuksien määrittelyä ja niiden tarkastusta yhteyden otossa, vastasoittojärjestelmää ja tiedon salakirjoittamista.

Paikallis- ja lähiverkkoihin kytkeytyminen on teknisesti yksinkertaista ja suhteellisen vaikeasti havaittavissa. Riskiä lisää yhteyksien helppo kohdennettavuus, esim. sabotaasin uhka on suurempi. Valvonnan ja fyysisten turvallisuustoimenpiteiden merkitys korostuu varsinkin verkkojen solmukohdissa. Kansainväliset tietoliikenneyhteydet hoidetaan yleensä linkki- ja satelliittiyhteyksin, jolloin salakuuntelun ja sanomien sieppauksen riski kasvaa.

Tietoliikenteessä tietoturvan merkitys korostuu mentäessä oman organisaation ulkopuolelle, jolloin oman organisaation mahdollisuudet vaikuttaa tietoturvallisuuteen heikentyvät. Tällöin korostuu palveluiden toimittajien ja yhteistyökumppanien valinta.

8
YHTEENVETO

Taloudellinen tilanne sekä tietoturvallisuusasioiden priorisointi suhteessa muihin kehittämistoimiin ovat aiheuttaneet sen, että turvasuunnitelmissa esitetyt turvatoimet ovat monasti siirretty myöhempään toteuttamisajankohtaan. Useissa organisaatioissa tietoturvallisuus on ensimmäisiä asioita joissa säästetään ja tämän vuoksi organisaatiossa otetaan suuriakin tietoisia riskejä. Mielenkiintoista kuitenkin on se, että tietoturva nähdään organisaatioissa tärkeänä osa-alueena, mutta siihen ei välttämättä haluta panostaa. Voidaan sanoa, että tietoturvan käsite esiintyy lähes kaikkien yritysten tietojärjestelmiä koskevissa suunnitelmissa ja strategiapapereissa, mutta varsinaiset tietoturvatoimenpiteet ovat usein jääneet vähäisiksi.

Verkottumisen ja tietojärjestelmien hajauttamisen myötä tietoturvan kohteet ja uhat ovat myös muuttuneet. Keskustietokonepohjaiset tietoturvasuunnitelmat kohdistuvat usein suurempiin hallinnollisiin kokonaisuuksiin, joiden alla saattaa kuitenkin olla kymmeniä tietoturvan kannalta merkittävä yksiköitä tai toimintoja, joiden tietoturvallisuuden tilaa on hajauttamisen myötä tuskin lainkaan selvitetty. Vaikka yksikön ylimmällä tasolla tietoturvallisuusasiat olisivatkin kunnossa, ei asia välttämättä ole sama alemmilla tasoilla ja päinvastoin.

Näyttää siltä, että politiikkatasolla (tietoturvapolitiikka, tietoturvallisuuspäätökset) organisaatioiden tietoturvallisuusasiat on pääpiirteittäin hoidettu, mutta käytännön toteutus on vielä kaukana tavoitetasosta. Yleensä tietotekniikan suurkäyttäjät huolehtivat myös tietoturvallisuudesta keskivertoa paremmin ja muilla tietoturvallisuusasiat ovat

enemmän tai vähemmän sattumanvaraisia ja keskittyneet pääasiassa vain joihinkin tietoturvan osa-alueisiin, kuten varmuuskopiointi tai virustorjunta[50]. Yleensä puutteet liittyvät vastuukysymyksiin ja organisointiin. Mikäli vastuuta turvatoimista, ohjeistuksesta, organisoinnista ja valvonnasta ei politiikkatasolla ole määritetty, ei vastaavia toimia myöskään ole suoritettu.

Tietoturvallisuus mielletään yleensä omaksi erilliseksi kokonaisuudeksi tietojenkäsittelyssä ja sen kehittämisessä. Organisaatioissa oletetaan, että tietoturva voidaan saavuttaa yksittäisillä projekteilla tai tehtävillä; virustorjunta, varmuuskopiointi, tietoturvaohjeet jne. Nämä toimenpiteet kuuluvat tietoturvaan, mutta tärkeintä olisi ensin huomata, ettei tietoturva ole erillinen toiminto, vaan olennainen ja kiinteä osa koko tietojenkäsittelyä ja sen kehittämistä. Parhaiten tietoturvaa voidaan kehittää ja ylläpitää tarkastelemalla turvallisuutta laadun näkökulmalta: tietoturva on osa tietojärjestelmän laatua. Tästä näkökulmasta katsottuna tietoturva tulee mukaan niin ylläpidossa kuin kehittämisprojekteissa. Tietoturvan tavoitteet tulevat suoraan tietojärjestelmälle asetetuista laatutavoitteista ja silloin resursseja voidaan ohjata tietoturvalle yleisen tietojärjestelmäkehityksen myötä.

---

[50] Valtionhallinnon tietoturvallisuuden johtoryhmä, s. 2

LÄHDELUETTELO

KIRJAT

Arnkil Lars, Christensen Kari, Heinonen Taisto, Hulkkonen Matti, Jaakkola Aimo, Mattila Tuomo, Mäkinen Matti, Neuvonen Kai — Tietosuojan toteuttamisohjeet:tutkimusraportti. Työryhmä:, Tietojenkäsittelyliitto Ray. julkaisu n:o 39, Kouvolan Kirjapaino 1979.

Booth, Grayce — Hajautetut systeemit. Kirjayhtymä Oy, Helsinki 1984.

Ekberg, Jan — Tietojärjestelmien suojaus. Valtion teknillinen tutkimuskeskus. Tiedotteita 802, Espoo 1987.

Ernst & Whinney — U.S. Computer Security Survey 1987

Ettala, Juha — Riskienhallintastrategia, 1986

Grimson, Jane & Kugler, Hans-Jörgen — Computer Security: the practical issues in a troubled world. IFIP/Sec'85, Elsevier Science Publishers B.V., Amsterdam 1985.

Garcia, Abel — Computer Security, a comprehensive controls checklist. John Wiley & Sons, New York 1986.

Hearnden, Keith — A handbook of computer security. Kogan Page Ltd, London 1987.

Kainomaa, Seppo — Tietoturva sekä vahingot ja väärinkäytökset atk:ssa. Tietotekniikan kehittämiskeskus r.y., tutkimusraportti 3/84. Helsinki, 1984.

Lane, V. P. — Security of computer based' information systems. Camelot Press Ltd, Southampton 1985.

Ledell & Roman & Voutilainen — Tietosuojaopas - mikrotietokoneiden käyttäjille. Mäntän kirjapaino Oy, Mänttä 1985.

Peltonen, Seppo — Tiedonhallinta. Tietoportti, Kouvola 1989.

Pohjola-yhtiöt — Tietoriskit, Pohjola-yhtiöiden julkaisuja 1, Hki 1991.

Saari, Juhani — Tietoturvallisuuden käsikirja. Otava, Keuruu 1988.

Saddington, Tricia — Security for small computer systems : a practical guide for users. Redwood Brun Ltd, Trowbridge, Wiltshire 1988.

Salonen Pekka — Tietoliikenneyhteyksien varimistaminen, HPY Konsultointi, Hki 1992

Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu — Puolustustaloudellinen suunnitelukunta, Valtionvarainministeriön järjestelyosasto 1989, Valtion painatuskeskus, Hki 1989

Tietoturvaopas — Yrittäjille ja muille pientietokoneiden käyttäjille. Yrittäjän Fennia, Helsinki 1989.

Wong, K. K. — Computer security. Risk analysis and control. A guide for the dp manager. NCC, Southampton 1987.

ARTIKKELIT

Adney, William & Kavanagh, Douglas — The Data Bandits. Byte 1989 : 1, 267 270.

Brown, Bob — The Small Data Center. Byte 1989 : 6, 286 - 287

Dror, Asael — Secret Codes. Byte 1989 : 6, 267 - 270.

Highland, Harold Joseph — Random Bits & Bytes, Network Communications Security. Computers & Security 1989 : 8, 553 - 561.

Jamieson, Richard & Low Graham — Security and Control Issues in Local Area Network Design. Computers & Security 1989 : 8, 305 - 316.

Moulton, Rolf — Network security. Datamation 1983 : 6, 121 - 122, 124.

Parker, Robert — Microcomputers Security and Control. The EDP Auditor Journal 1988 : 1, 13 - 20.

Saari, Juhani — Atk-järjestelmien virukset ja niiden torjunta. Tilintarkastus 1989 : 3, 188 - 192.

Sjöström, Mikael — Käyttäjät mukaan tietoturvan suunnitteluun. Tekniikka & Talous 29.8.1990, s. 11

Stephenson, Peter — Personal and Private. Byte 1989 : 6, 285 - 288.

Tate, Paul — Risk! The third factor. Datamation 1988 : 4, 58 - 64.

Wood, Charles Cressson — Planning: A Means to Achive Data Communications Security. Computers & Security 1989 : 8, 189 - 199.

Zajac Jr.,Bernard — Distributed data processing: New problems. Computers & Security 1988 : 7, 249 -250

Tuhoojavirukset iskeneet suomalaisiinkin tiedostoihin. — Helsingin Sanomat 5.3.1990, s. 7

Uusitupa, Seppo — Tietoturvaa - miksi ja miten. Tietokone 1989 : 10, 54 - 55.

Valtionhallinnon tietoturvallisuuden johtoryhmä — Tietoturvallisuuden tilannekartoitus, tilanneraportti 15.7.1994 s. 1 - 3